Miika Rinne

Langattoman lähiverkon toteutus keskitetyllä verkonhallintajärjestelmällä

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

10.5.2016

Metropolia

Tekijä Otsikko Sivumäärä Aika	Miika Rinne Langattoman lähiverkon toteutus keskitetyllä verkonhallinta-järjestelmällä 48 sivua + 1 liite 10.5.2016
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja	Yliopettaja Matti Puska

Insinöörityön tavoitteena oli perehtyä erään yhdysvaltalaisen verkkolaitevalmistajan reitittimen ja langattoman tukiaseman käyttöönottoon sekä hallintaan, toteuttamalla kuvitteelliselle yritykselle yksinkertainen lähiverkko. Työntekijöille luotiin oma langaton verkkotunnus, ja vierailijat sijoitettiin omaan eristettyyn verkkosegmenttiin.

Reitittimeen on asennettu avoimeen lähdekoodiin perustuva, mutta nykyään laitevalmistajan itsensä kehittämä, Linux-pohjainen käyttöjärjestelmä. Intuitiivisen web-käyttöliittymän avulla pystytään konfiguroimaan suurin osa reitittimen toiminnollisuudesta, mutta saatavilla on myös komentoriviliittymä. Reitittimen nopea ja tehokas käyttöönotto onnistuu parhaiten sen käyttöönottoapurilla. Käyttöönottoapurin tekemiä määrittelyjä ja palomuurisääntöjä tutkittiin, ja todettiin niiden olevan yleiseen tarpeeseen sopivia.

Tukiasema kuuluu yhtenäistettyyn tuoteperheeseen, jota hallinnoidaan yrityksen omalla ohjelmistopohjaisella verkonhallintajärjestelmällä eli kontrollerilla. Kontrolleri kerää tietoa verkon käytöstä ja käyttäjistä, ja sen avulla voidaan suorittaa konfiguraatiomuutoksia ja firmware-päivityksiä useampaan tuoteperheen laitteeseen kerralla. Tuoteperhettä markkinoidaan ohjelmisto-ohjattuna verkkoratkaisuna (SDN, Software-Defined Networking). Tutkimuksessa kuitenkin selvisi, etteivät laitteet tue yleisiä SDN-protokollia. Ohjaus- ja tiedonvälityskerros on toteutettu laitteissa itsessään. Kontrolleri suorittaa laitteisiin tehtävät muutokset SSH-yhteyden välityksellä.

Työn lopputuloksena saatiin toimiva verkkoympäristö, ja sivutuotteena syntyi ohjeistus laitteiden käyttöönotosta ja kuvaus ominaisuuksista.

Avainsanat	Ubiquiti, EdgeOS, UniFi, EdgeRouter, kontrolleri

Author Title Number of Pages Date	Miika Rinne Implementing a wireless LAN using a network management system 48 pages + 1 appendix 10 May 2016
Degree	Bachelor of Engineering
Degree Programme	Information and Communications Technology
Specialisation option	Data Networks
Instructor	Matti Puska, Principal Lecturer

The purpose of this final year project was to study the deployment and management of a router and a wireless access point by implementing a local area network for an imaginary enterprise. The network devices are manufactured by a US-based company.

The router has a Linux-based operating system installed. The operating system is currently developed and maintained by the manufacturer itself. Most of the router's functionality is configurable through the router's intuitive web interface, but a command-line interface is also available. The fastest way to deploy the router is through one of its setup assistants. Configuration changes made by the setup assistant were examined and discovered to be secure and suitable for general needs.

The wireless access point is a part of a unified product family, which is controlled by a software-based network management system, a controller. The controller collects network usage statistics, and it is possible to make configuration changes and firmware-upgrades to multiple devices at once by using it. The controller makes the changes through an SSH connection. The product family is marketed as a software-defined networking solution. However, it was discovered that the devices of the product family do not support any of the SDN protocols. The control and data plane are implemented in the devices themselves.

As a result, a successfully working network environment was created. Guidance for the deployment and a description of the devices' features were produced as a side product.

Keywords	Ubiquiti, EdgeOS, UniFi, EdgeRouter, controller

Sisällys

Lyhenteet ja käsitteet

AES	*Advanced Encryption Standard.* Lohkosalausmenetelmä.
ARP	*Address Resolution Protocol.* Verkkoprotokolla, jolla selvitetään IP-osoitetta vastaava MAC-osoite.
BGP	*Border Gateway Protocol.* Dynaaminen reititysprotokolla.
DHCP	*Dynamic Host Configuration Protocol.* Verkkoprotokolla, joka jakaa IP-osoitteita verkon päätelaitteille.
DNS	*Domain Name System*. Nimipalvelinjärjestelmä, joka muuttaa verkkotunnukset IP-osoitteiksi.
EAP	*Extensible Authentication Protocol*. 802.1X-todennuksessa käytetty tunnistusprotokolla.
FCC	*Federal Communications Commission.* Yhdysvaltain telehallintovirasto.
IEEE	*Institute of Electrical and Electronics Engineers.* Kansainvälinen tekniikan alan järjestö, jonka tehtäviin kuuluu muun muassa tietoverkkostandardien määrittely.
ISP	*Internet Service Provider.* Palveluntarjoaja, esimerkiksi teleoperaattori.
IV	Initialization Vector. Alustusvektori.
LAN	*Local Area Network.* Lähiverkko.
LED	*Light-emitting diode.* Puolijohdekomponentti, joka säteilee valoa.
MAC	*Media Access Control.* Jokaisella verkkokortilla on yksilöllinen MAC-osoite.
MIPS	*Microprocessor without Interlocked Pipeline Stages.* MIPS-prosessoriarkkitehtuuri
MPLS	*Multiprotocol Label Switching.* Protokolla, jolla kuljetetaan paketteja nopean runkoverkon kautta ilman reititystä.
NAT	*Network Address Translation.* Osoitteenmuunnos.

NMS	*Network Management System.* Verkonhallintajärjestelmä, jossa hallintakerros on eriytetty ohjaus- ja tiedonvälityskerroksesta.
OSPF	*Open Shortest Path First*. Dynaaminen reititysprotokolla.
PD	*Powered Device.* PoE-virransyöttöä vastaanottava laite.
PoE	*Power over Ethernet.* Tekniikka, jonka avulla voidaan sähköä siirtää parikaapelissa.
PSE	*Power-Sourcing Equipment.* PoE-virransyötän lähdelaite.
PSK	*Pre-shared-Key.* Ennalta jaettu avain, jota käytetään todentamismenetelmänä WPA ja WPA2-protokollissa.
RADIUS	*Remote Authentication Dial-In User Service.* Käyttäjien keskitettyyn todentamiseen tarkoitettu protokolla.
SDN	*Software-Defined Networking.* Ohjelmisto-ohjatut verkot.
SNMP	*Simple Network Management.* Verkonhallintaprotokolla.
SSH	*Secure Shell.* Suojattu etäyhteys.
SSID	*Service Set Identifier*. Langattoman verkon tunnus.
TCP	*Transmission Protocol.* Protokolla, jolla luodaan yhteys tietokoneiden välille.
TKIP	*Tempory Key Integrity Protocol.* RC4-algoritmiin pohjautuva langattoman verkon salausmenetelmä.
TLS	*Transport Layer Security.* Salausprotokolla.
VLAN	*Virtual Local Area Network.* Tekniikka, jolla verkko voidaan jakaa eri kokoisiin loogisiin osiin.
VoIP	*Voice over IP.* Äänen reaaliaikaiseen siirtämiseen verkon välityksellä käytetty protokolla.
WAN	*Wide Area Network.* Laajaverkko, jonka on yleensä toteuttanut jokin teleoperaattori.

WEP	*Wired Equivalent Privacy.* WEP-salaus, joka on nykyään poistunut käytöstä sen haavoittuvuuksien takia.
WISP	*Wireless Internet Service Provider.* Langattoman laajakaistan palveluntarojaja.
WLAN	*Wireless Local Area Network.* Langaton lähiverkko.
WPA	*Wi-Fi Protected Access.*
WWW	*World Wide Web.* Tarkoittaa Internetiä. Tässä raportissa se viittaa UniFi-kontrollerissa esiintyvään symboliin, joka ilmaisee Internet-yhteyden tilaa.

1 Johdanto

Insinöörityön tavoitteena on toteuttaa kuvitteelliselle yritykselle langaton lähiverkko käyttämällä verkkolaitevalmistaja Ubiquiti Networksin EdgeRouter X -reititintä ja UniFi AP LR -tukiasemaa. Nykypäivän yrityksissä on hyvin yleistä tarjota pääsy Internetiin myös vierailijoille ja yhteistyökumppaneille. Yhtenä tutkimuksen kohteena ovat ominaisuudet ja menetelmät, joiden avulla pystytään mainituilla laitteilla toteuttamaan muusta sisäverkosta eristetty vierailijaverkko.

Raportissa perehdytään yleisellä tasolla Ubiquiti Networksiin ja sen tuoteperheisiin. UniFi-tuoteperhettä on markkinoitu ohjelmisto-ohjattuna verkkoratkaisuna. Työssä selvitetään, miten laitteiden hallinnointi on toteutettu, tutustumalla lyhyesti erilaisiin verkonhallintaratkaisuihin. Raportin ensimmäisissä luvuissa esitellään tietoverkkoihin liittyviä standardeja ja verkon tietoturvallista toteutusta. Ubiquitin tuotteet ovat kohtuuhintaisia, joten kuluttajatkin voivat niitä hankkia. Tästä syystä työssä selvitetään, kuinka helppoa niiden käyttöönotto on.

Sain idean insinöörityöhön, kun korvasin oman kotiverkkoni reitittimen Ubiquitin EdgeRouter Litellä. Tiesin laitteesta ennalta vain sen, että siihen on asennettu Linux-pohjainen käyttöjärjestelmä. Koska jouduin joka tapauksessa syventymään laitteen toimintaan, päätin samalla dokumentoida prosessin. Tein hieman taustatutkimusta ja huomasin, että laajempaa Ubiquitin tuotteisiin keskittyvää insinöörityötä ei vielä ollut tehty, mikä vahvisti päätöstäni ja motivoi aloittamaan insinöörityön tekemisen. Työn tuloksia voidaan hyödyntää esimerkiksi yritysverkkojen suunnittelussa ja toteutuksissa.

Testattavat laitteet lainasi Pietarsaaressa toimiva Noyra Oy, joka myy Ubiquitin tuotteita ja konsultointipalveluita Suomessa. Yritys on testannut laitteiden toimintaa jo usean vuoden ajan ja tarjoaa pienelle testiryhmälle laajakaistapalveluita Pietarsaaressa WISP-palveluna (Wireless Internet Service Provider) Ubiquitin laitekantaa ja teknologiaa hyödyntäen. Lisäksi yritys on liittänyt Ubiquitin langattomia jakelulinkkejä avoimeen tietoliikenneverkkoon. (1; 2.)

2 Lähiverkot

Lähiverkolla (LAN, Local Area Network) tarkoitetaan maantieteellisesti pienelle alueelle sijoittuvaa, yleensä yhden organisaation hallussa olevaa tietoverkkoa, joka koostuu reitittimistä, kytkimistä, langattomista tukiasemista (WLAN, Wireless Local Area Network) ja päätelaitteista. Laajaverkoiksi (WAN, Wide Area Network) kutsutaan laajempia verkkokokonaisuuksia, jotka ulottuvat paikkakunnalta toiselle tai maan rajojen ulkopuolelle. Laajaverkot on yleensä toteuttanut jokin teleoperaattori, ja ne yhdistävät lähiverkot toisiinsa. (3, s. 4–5.)

Lähiverkko eli sisäverkko tulee olla erotettuna julkisesta verkosta eli Internetistä palomuurilla. Sisäverkkoa on tämän lisäksi syytä jakaa pienempiin osiin verkon toiminnan ja tietoturvan parantamiseksi. Yleinen hyvä periaate on jakaa eri toiminnot ja laitteet omiin verkkoalueisiin, kuten esimerkiksi langaton verkko erilleen langallisesta verkosta. Verkko tulee jakaa vähintään erillisiin virtuaalisiin verkkoihin eli VLAN:eihin (Virtual Local Area Network), jotta liikennettä voidaan tarpeen tullen rajoittaa palomuurisäännöillä. (4, s. 484.)

2.1 Verkkolaitteiden hallinta

Luvussa käydään läpi verkkolaitteiden erilaisia hallintamalleja ja esitellään yleisellä tasolla tulevaisuuden kehityssuuntia, joihin kuuluvat muun muassa ohjelmisto-ohjatut verkot.

2.1.1 Loogiset toimintakerrokset

Verkkolaitteen sisäinen toiminta on perinteisesti jaettu kolmeen toiminnalliseen kerrokseen, hallintakerrokseen (Management Plane), ohjauskerrokseen (Control Plane) ja tiedonvälityskerrokseen (Data Plane). Hallintakerros saattaa joissain teknisissä toteutuksissa ja asiayhteyksissä olla yhdistettynä ohjauskerrokseen.

Hallintakerrokseen sisältyy monitorointi- ja hallinnointiominaisuuksia. Yksi esimerkki hallintakerroksen ratkaisusta on verkonhallintajärjestelmä (NMS, Network Management System).

Ohjauskerros määrittää, kuinka paketit verkossa liikkuvat ja mitä protokollia pakettien siirtoon käytetään. Ohjauskerrosta nimitetään verkon älykkyydeksi, ja se on perinteisesti sijainnut verkkolaitteissa itsessään. Tyypillisen reitittimen ohjauskerroksen protokolliin kuuluu esimerkiksi dynaamiset reititysprotokollat OSPF (Open Shortest Path First) ja BGP (Border Gateway Protocol).

Tiedonvälityskerros vastaa pääasiallisesti vain pakettien siirrosta, kun ohjauskerros on määrittänyt, mihin ne siirretään. Yksittäinen reititin on esimerkki sijainnista, jossa tiedonvälityskerros toimii.

Verkon arkkitehtuurista ja laitevalmistajasta riippuen on eroavaisuuksia tavoissa, miten nämä kolme loogista toiminnan kerrosta on toteutettu. Perinteisessä autonomisessa hallintamallissa kaikki kerrokset sijaitsevat yhdessä laitteessa. Nykypäivänä kerrokset voivat kuitenkin olla hajautettuna erillisiin laitteisiin, kontrollereihin ja pilvipalveluihin. (4, s. 337–339.)

2.1.2 Autonominen hallinta

Autonomisessa hallintamallissa kaikki kolme loogista kerrosta sijaitsevat yhdessä fyysisessä laitteessa. Kuluttajille suunnatuissa laitteissa on monesti kolme laitetta: reititin, kytkin ja langaton tukiasema yhdistettynä yhteen laitteeseen. (4, s. 380.)

Yksi monista haasteista langattomien tukiasemien ja yleensäkin verkkolaitteiden hallinnassa on niiden suuri määrä. Autonomisen hallintamallin yhtenä huonona puolena on, että jokainen laite pitää konfiguroida erikseen. Tämän ongelman ratkaisemiseen on kehitetty erilaisia keskitettyjä hallintaratkaisuja. (4, s. 399, 341.)

2.1.3 Keskitetty hallinta

Verkonhallintajärjestelmä on yksi esimerkki keskitetystä hallintaratkaisusta, jonka ominaisuuksiin kuuluu mahdollisuus monitoroida laitteiden antamia ilmoituksia ja hälytyksiä. NMS-ratkaisut ovat yleensä laitevalmistakohtaisia, mutta myös avoimen lähdekoodin vaihtoehtoja on olemassa. NMS kommunikoi hallinnoitavien laitteiden kanssa erilaisten hallinnointiprotokollien kuten SNMP:n (Simple Network Management Protocol) avulla. NMS on hallintakerroksen ratkaisu, joten kaksi muuta kerrosta toteutetaan edel-

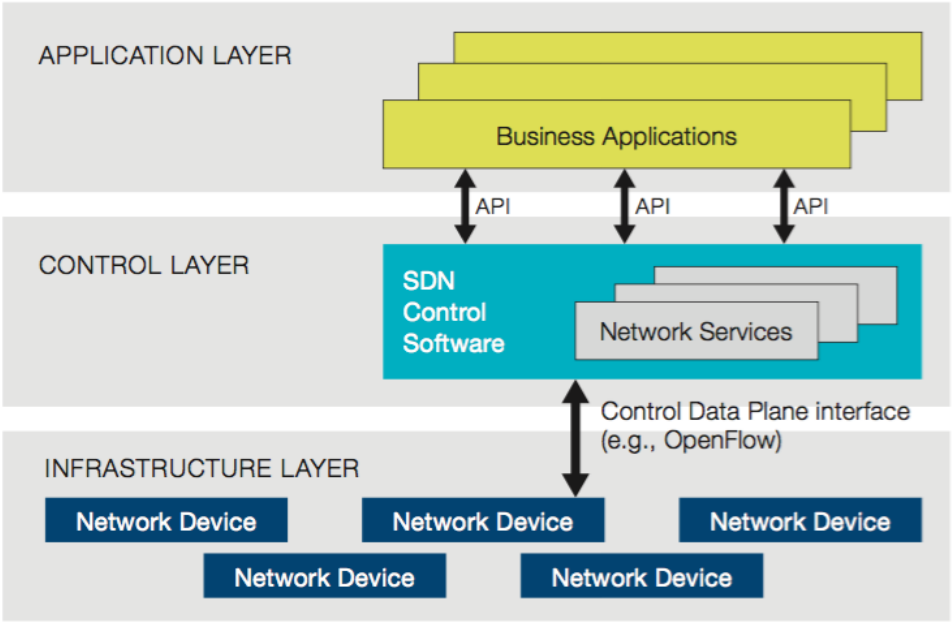
leen laitteissa itsessään. NMS:n avulla voidaan monitoroida myös langallisen ja langattoman verkon käyttäjiä. NMS-tyyppisiä ratkaisuja pystytään sijoittamaan esimerkiksi pilvipalveluun. (4, s. 341–343.)

Vuoden 2002 alussa monet langattomien verkkolaitteiden valmistajat päättivät siirtyä keskitettyyn WLAN-kontrolleriratkaisuun, jossa kaikki kolme toiminnallista kerrosta sijaitsisivat yhdessä keskitetyssä laitteessa. Kuormituksen tasapainotus (load balancing) ja vaeltelu (roaming) toteutettaisiin tukiasemien sijaan kontrollerissa. Tämäntyyppisessä ratkaisussa päätelaiteliikenne yleensä ohjataan jollain tunnelointiprotokollalla kontrolleriin. WLAN-kontrollereita nimitetään usein langattomiksi kytkimiksi, koska ne välittävät tietoa verkon siirtokerroksessa (Layer 2). Monet WLAN-kontrollerit ovat kuitenkin monitasokytkimiä, koska ne pystyvät myös reitittämään liikennettä verkkokerroksessa (Layer 3). Laitevalmistajilla saattaa olla omia protokollia, joiden avulla tukiasemien ja kontrollerin välinen liikenne on toteutettu. (4, s. 343–345.)

2.1.4 Ohjelmisto-ohjatut verkot

Sosiaalinen media, mobiililaitteet ja pilvipalvelut venyttävät perinteisiä tietoverkkoja äärirajoille. Ohjelmisto-ohjattujen verkkojen tarkoitus on antaa verkkoylläpitäjille mahdollisuus vastata nopeasti muuttuviin liiketoiminnan vaatimuksiin keskitetyn verkonhallinnan avulla. SDN-verkoissa ohjauskerros on keskitetty ohjelmistopohjaiseen SDN-kontrolleriin, joka ylläpitää kokonaiskuvaa verkon tilasta. SDN-verkkojen kehityksen tavoitteena on tarjota yritykselle ja palveluntarjoajille hallintaratkaisu, joka on laitevalmistajariippumaton. SDN-verkossa verkkolaitteiden ei enää tarvitse ymmärtää monimutkaisia protokollia, vaan pelkästään suorittaa SDN-kontrollerin antamat yksinkertaiset käskyt. (5; 6.)

Ylläpitäjät pystyvät nopeasti muuttamaan ja optimoimaan tietoverkkoa käyttämällä erilaisia automatisoituja SDN-ohjelmia, jotka ovat laitevalmistajariippumattomia, ja niitä voidaan tästä syystä kirjoittaa myös itse. SDN-verkkoratkaisujen tuottajat tarjoavat laajan valikoiman kilpailevia arkkitehtuureja, mutta yksinkertaisimmillaan SDN keskittää verkonhallinnan erottamalla ohjauskerroksen laitteista. SDN-ratkaisut sisältävät yleensä jonkinlaisen SDN-kontrollerin sekä Northbound- ja Southbound-ohjelmointirajapinnat (API, Application Programming Interface) (kuva 1). (6.)



Kuva 1. SDN-verkon toimintaperiaate (5, s. 7)

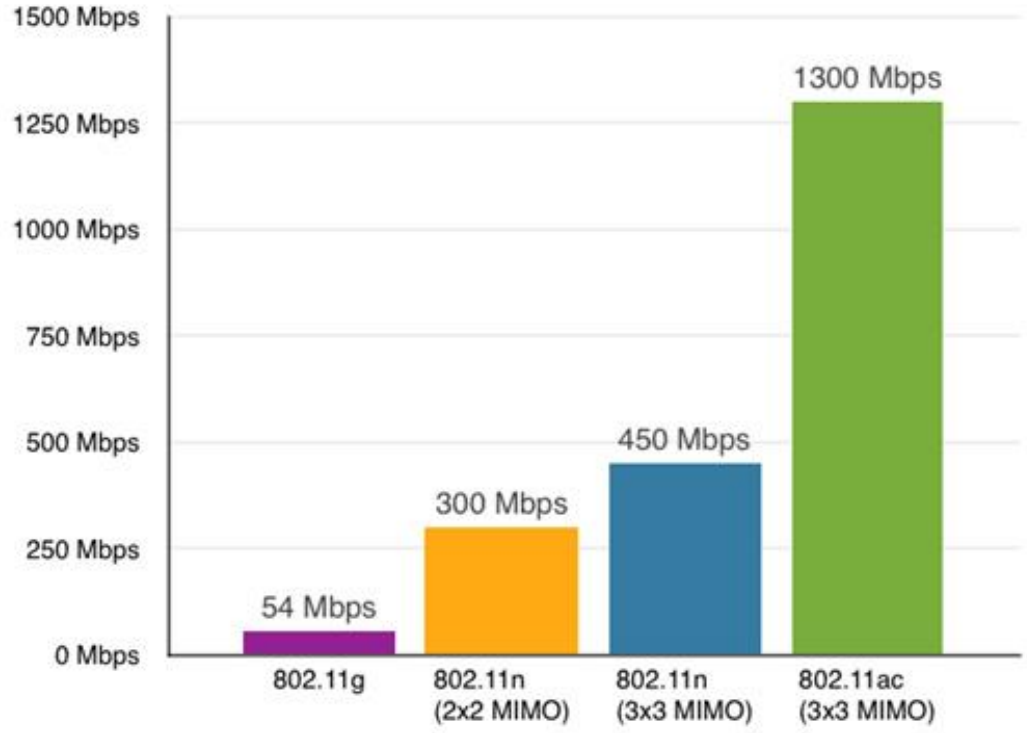
Northbound-rajapinta kommunikoi ”yläpuolella” olevien ohjelmien ja liiketoimintamallien kanssa, joita ylläpitäjät voivat käyttää ohjelmoidakseen verkkoliikenteen kulkua. Southbound-rajapinta välittää tietoa reitittimille ja kytkimille ”alapuolella”. OpenFlow oli yksi ensimmäisistä SDN-protokollastandardeista ja pysyy yhtenä käytetyimpänä. OpenFlow’ta pidetään yleensä synonyymina ohjelmisto-ohjatuille verkoille, vaikka se on vain yksi elementti SDN-arkkitehtuurissa. OpenFlow on avoin standardi, joka mahdollistaa ohjauskerroksen ja tiedonvälityskerroksen vuorovaikutuksen eikä suinkaan ole ainoa SDN-protokolla. (5; 6.)

2.2 Langattomat lähiverkot

IEEE (Institute of Electrical and Electronics Engineers) on kansainvälinen tekniikan alan järjestö, jolla on yli 400 000 jäsentä 160 maassa. Järjestön tehtävänä on luoda tietoverkkoja varten standardeja, joita kehitetään työryhmissä. 802.3-työryhmä vastaa Ethernet-standardeista ja 802.11-työryhmä langattomiin verkkoihin liittyvistä standardeista. Kun teknologian kehittyessä tulee tarve uudistaa standardeja, luodaan uusi tehtäväryhmä. Tehtäväryhmälle annetaan työryhmän nimi, mutta perään lisätään kirjain erottamaan uusi standardi vanhoista. 802.11n ja 802.11ac ovat esimerkkejä langattomien verkkostandardien tehtäväryhmistä. (4, s. 7–8.)

Wi-Fi–allianssi on globaali, voittoa tavoittelematon toimialajärjestö, jolla on yli 550 jäsenyritystä. Allianssi on omistautunut edistämään langattomien verkkojen yleistymistä ja varmistaa markkinoilla olevien langattomien laitteiden yhteensopivuuden Wi-Fi-sertifioinnin avulla. (4, s. 10–11.)

Tämän insinöörityön ymmärtämisen kannalta ei ole tarvetta paneutua syvällisesti 802.11-standardeihin. Erot tiedonsiirtonopeuksissa eri standardien välillä on kuitenkin tärkeää hahmottaa. Kuvassa 2 on vertailtu 802.11g/n/ac-standardien maksimaalisia tiedonsiirtonopeuksia. Korkeampi palkki tarkoittaa nopeampaa tiedonsiirtonopeutta. 802.11ac-standardi on tällä hetkellä nopein markkinoilla yleisesti tuetuista standardeista.



Kuva 2. 802.11g/n/ac-standardien maksimitiedonsiirtonopeuksien vertailu (7).

Langattomien lähiverkkojen tietoturva

Langattomat verkot käyttävät lisensoimattomia taajuuksia, joten kaikki verkkoliikenne kulkee avoimesti ilmassa. Tiedon turvaaminen langallisessa verkossa on jonkin verran helpompaa verrattuna langattomiin verkkoihin, koska langatonta tiedonsiirtoa voidaan helposti salakuunnella. Tästä syystä on tärkeää käyttää erilaisia salausalgoritmeja, joista kaksi yleisintä ovat symmetrinen jonosalaaja RC4 (Rivest Cipher 4) ja lohkosalausmenetelmä AES (Advanded Encryption Standard). (4, s. 462.)

WEP (Wired Equivalent Privacy) käyttää RC4-salausalgoritmia. 64-bittinen WEP-salaus muodostuu 40-bittisestä staattisesta avaimesta, joka yhdistetään 24-bittisen alustusvektorin (IV, Initialization Vector) kanssa. Alustusvektori on eri jokaisessa kehyksessä ja se lähetetään selväkielisenä. Erilaisia yhdistelmiä alustusvektorille on kuitenkin vain 16 777 216, minkä takia joudutaan käyttämään samoja arvoja uudestaan. Myöhemmin otettiin käyttöön 128-bittinen WEP-salaus, joka koostui 104-bittisestä staattisesta avaimesta ja myös 24-bittisestä alustusvektorista. WEP-salausta ei enää moneen vuoteen ole suositeltu käytettäväksi, sillä se pystytään parhaillaan murtamaan muutamassa minuutissa. (4, s. 468–469.)

TKIP (Temporal Key Integrity Protocol) -salaus perustuu myös RC4-algoritmiin. WEP-salauksen ongelma ei ollut RC4 vaan tapa, jolla salaus muodostettiin. TKIP käyttää 128-bittistä väliaikaista avainta, joka on yhdistetty 48-bittisen alustusvektorin sekä lähteen ja kohteen MAC-osoitteen (Media Access Control) kanssa. Tätä prosessia kutsutaan pakettikohtaiseksi avaimen sekoitukseksi. TKIP-salausta ollaan hiljalleen poistamassa käytöstä, eikä sitä enää tueta 802.11n/ac-standardien nopeuksilla. Taaksepäin yhteensopivuuden takia tukiasemissa tuetaan vielä TKIP- ja WEP-salauksia hitaammille 802.11a/b/g-standardeille. (4, s. 481–484.)

CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) -salaus hyödyntää AES-algoritmia, joka käyttää 128-bittistä salausavainta salaamaan 128-bittisiä kiinteänpituisia lohkoja. AES-algoritmin vahvuuden takia pakettikohtainen avaimen sekoitus ei ole tarpeellista, vaan kaikki CCMP-salausavaimet luodaan dynaamisesti neljävaiheisella kättelyllä (4-way handshake). AES/CCMP-salausta suositellaan käytettäväksi langattoman verkon suojaamiseen. (4, s. 482.)

WPA (Wi-Fi Protected Access) -protokolla tukee ainoastaan TKIP/RC4-salausta. Myöhemmin esiteltiin WPA2, joka tukee TKIP/RC4-salauksen lisäksi AES/CCMP-salausta. Ainoa ero WPA- ja WPA2-protokollan välillä on eri algoritmin käyttäminen salauksessa.

PSK (Preshared Key) eli ennalta jaettu avain on todentamismenetelmä, jota käytetään WPA- ja WPA2-protokollien kanssa. Wi-Fi-allianssin viralliset nimet menetelmälle on WPA-Personal ja WPA2-Personal. Laitevalmistajat käyttävät kuitenkin useita eri nimiä, kuten WPA/WPA2-PSK ja WPA/WPA2-Passphrase. Kaikki tukiasemat, jotka on valmistettu vuoden 2006 jälkeen ja saaneet WiFi-sertifioinnin, tukevat WPA2/PSK-todennusta AES/CCMP-salauksella. (4, s. 473–474.)

IEEE 802.1X on standardi porttikohtaiselle pääsynvalvonnalle, jota käytetään yleisesti yritysympäristöissä, ja se voidaan toteuttaa sekä langalliselle että langattomalle verkolle. Toteutuksissa käytetään yleensä RADIUS (Remote Authentication Dial In User Service) -palvelinta. Päätelaitteesta, joka pyytää todennusta verkkoon, käytetään nimitystä anoja (supplicant). Jokaisella anojalla on ainutlaatuiset kirjautumistiedot, jotka varmistetaan todennuspalvelimelta (authentication server). Todentaja (authenticator), joka on esimerkiksi kytkin tai tukiasema, sallii tai evää päätelaitteen pääsyn verkkoon varmistamalla kirjautumistiedot todennuspalvelimelta. Todentamiseen käytetään EAP-protokollaa (Extensible Authentication Protocol), jonka toimintaa ei käsitellä sen syvemmin tässä insinöörityössä. (4, s. 474–477.)

Taulukossa 1 on vielä esitetty selkeämmin langattomien verkkojen eri todennus- ja salausmenetelmät.

Taulukko 1. Langattoman verkon todennus- ja salausmenetelmät (4, s. 471).

Wi-Fi-allianssin sertifioima nimi	**Todennus**	**Salaus**	**Salausalgoritmi**	**Avaimen muodostus**
	Jaettu avain	WEP	RC4	Staattinen
WPA-Personal	WPA/PSK	TKIP	RC4	Dynaaminen
WPA-Enterprise	802.1X/EAP	TKIP	RC4	Dynaaminen
WPA2-Personal	WPA2/PSK	CCMP (suositeltu) TKIP (ei suositeltu)	AES (suositeltu) RC4 (ei suositeltu)	Dynaaminen
WPA2-Enterprise	802.1X/EAP	CCMP (suositeltu) TKIP (ei suositeltu)	AES (suositeltu) RC4 (ei suositeltu)	Dynaaminen

2.3 Power over Ethernet -tekniikka

Power over Ethernet (PoE) -tekniikka mahdollistaa sähkön ja datan siirtämisen samalla parikaapelilla muun muassa VoIP-puhelimille (Voice over IP), valvontakameroille ja langattomille tukiasemille, mikä vähentää asennuskustannuksia ja lisää joustavuutta laitteiden sijoittelun suhteen. Parikaapeli koostuu neljästä johtoparista, joista kahta paria käytetään datan siirtämiseen 10/100 Mb/s-nopeuksilla. Kaikki neljä johtoparia tarvitaan datan siirtämiseen nopeudella 1 Gb/s. Sähköä pystytään syöttämään käyttämättömissä johtopareissa (mode B) ja datan siirtämiseen käytetyissä johtopareissa (mode A).

IEEE määritteli PoE-tekniikan alun perin 802.3af-standardissa vuonna 2003. 802.3af-yhteensopivan päätelaitteen suurin tehontarve saa olla 15,4 W. Parikaapelissa ilmenevien häviöiden takia vain 12,95 W on taattu tehon määrä. IEEE 802.3at-standardi, joka tunnetaan myös nimellä PoE plus (PoE+), ratifioitiin vuonna 2009. Standardin päätarkoitus oli laajentaa PoE-tekniikan sähkönsyöttöominaisuuksia, mutta samalla säilyttää taaksepäin yhteensopivuus. 802.3at-standardin mukaan päätelaitteen suurin tehonkulutus saa olla korkeintaan 25,5 W. (4, s. 597.)

PoE-standardissa määritellään kaksi laitetyyppiä: virran vastaanottavat päätelaitteet (PD, Powered Device) ja virran syöttävät lähdelaitteet (PSE, Power-Sourcing Equipment). Päätelaitteet ovat yleensä tukiasemia, lähdelaitteet kytkimiä (kuva 3) tai erilaisia injektoreita (kuva 5).

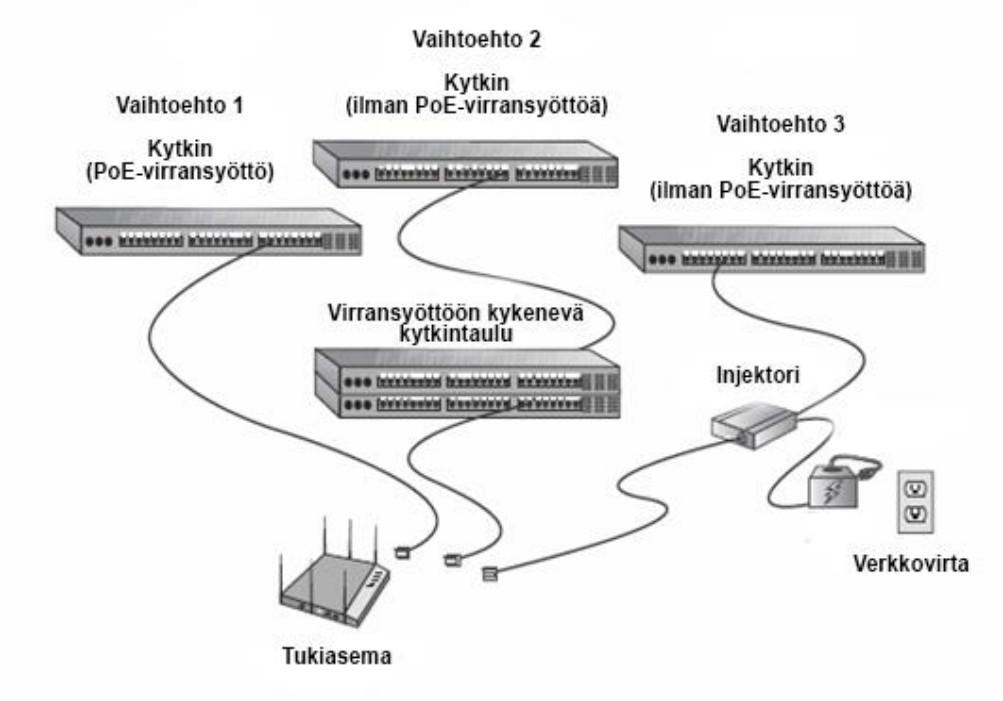
Kuva 3. 802.3af- ja 802.3at-yhteensopiva 24-porttinen UniFi Switch -kytkin.

Standardin mukaisen päätelaitteen täytyy pystyä vastaanottamaan virtaa 57 V:n jännitteellä. Lähdelaite pyrkii havaitsemaan, onko siihen kytketty päätelaite kykenevä virran vastaanottoon, lähettämällä sille tunnistussignaalin (detection signal). Päätelaitteen

tulee pystyä vastaamaan tunnistukseen havaitsemisallekirjoituksella (detection signature), mikä ilmaisee päätelaitteen olevan standardin mukainen. Jos päätelaite ei vastaa tunnistussignaaliin, lähdelaite ei syötä sille virtaa. Näin estetään yhteen sopimattoman päätelaitteen vaurioituminen. Riippuen valmistajasta ja lähdelaitteesta on kuitenkin mahdollista, että virran vastaanottoon kykenevän laitteen irrottamisen jälkeen, virta kulkee parikaapelissa vielä muutamia sekunteja. Jos jokin virran vastaanottoon kykenemätön laite liitetään tässä ajassa lähdelaitteeseen, saattaa liitetty laite vahingoittua. Tästä syystä on hyvä odottaa aina noin kymmenen sekuntia ennen uuden laitteen liittämistä lähdelaitteeseen. (4, s. 598–600, 612–613.)

Lähdelaitteet on jaettu pääasiallisiin (Enspan PSE) ja välimallin (Midspan PSE) lähdelaiteisiin. Pääasialliset lähdelaitteet ovat yleensä kytkimiä, jotka kykenevät neuvottelemaan virransyötön tarpeen ja virran määrän. Välimallin lähdelaite toimii yleensä vain virran välittäjinä (pass-through) ja datan toistimena (repeater). (4, s. 596–603.)

Kuvassa 4 nähdään eri vaihtoehtoja syöttää virtaa PoE-tekniikkaan kykenevälle tukiasemalle. Ensimmäisessä vaihtoehdossa virta syötetään PoE-kytkimellä, seuraavassa vaihtoehdossa virransyöttöön kykenevällä kytkentätaululla ja viimeisessä vaihtoehdossa on käytetty injektoria.



Kuva 4. Kolme vaihtoehtoa syöttää virtaa PoE-tekniikkaan kykenevälle laitteelle (4, s. 608).

Passive PoE

Passiiviset lähdelaitteet (Passive PoE) eivät ole 802.3af- ja 802.3at-standardien mukaisia, eivätkä ne kykene neuvottelemaan virransyötön tarpeellisuudesta. Passiviinen lähdelaite syöttää virtaa päätelaitteelle, oli se sitten kykenevä vastaanottamaan virtaa tai ei, mikä saattaa vaurioittaa vastaanottoon kykenemättömiä päätelaitteita. Passiivinen lähdelaite (kuva 5) on halvempi ratkaisu valmistaa ja toteuttaa, minkä takia useimmat laitevalmistajat käyttävät sitä. (8; 9.)

Kuva 5. Useimmat Ubiquitin Networksin PoE-injektorit ovat Passive PoE -tyyppisiä.

3 Ubiquiti Networks

3.1 Tietoa yrityksestä

Ubiquiti Networks on yhdysvaltalainen verkkolaitevalmistaja, jonka erikoisalaan kuuluvat langattomat jakelulinkit. Yrityksen perusti Robert J. Pera vuonna 2005. Hän on vielä tänäkin päivänä yrityksen toimitusjohtaja ja suurin osakkeenomistaja yli 65 %:n osuudellaan. Yrityksen nimi tulee sanasta ubiquitous, joka tarkoittaa kaikkialla läsnä olevaa. Peran mukaan nimi kertoo yrityksen visiosta tuoda Internet-yhteys kaikkien saataville. Yritys työllistää hieman yli 430 työntekijää, ja sen pääkonttori sijaitsee San Josessa Yhdysvalloissa. Vuonna 2015 yrityksen liikevaihto oli 600 miljoonaa dollaria. (10; 11; 12; 13.)

Ennen yrityksen perustamista Pera työskenteli kaksi vuotta teknologiayritys Applella langattomien tukiasemien testauksen parissa. Hänen tehtävänään oli varmistaa, että tukiasemat noudattavat Yhdysvaltain telehallintovirasto FCC:n (Federal Communications Commission) elektromagneettiselle säteilylle asettamia standardeja. Tukiasemia testatessaan Pera huomasi säteilyarvojen olevan huomattavasti sallittujen raja-arvojen alapuolella ja lisäämällä lähetystehoa voitaisiin yhteydelle saavuttaa pidempi kantama. Applen jätettyä kehitysidean huomiotta Pera päätti rakentaa oman prototyypin.

Tutkiessaan asiaa tarkemmin hän löysi useita tapauksia, joissa syrjäisillä seuduilla asuvat ihmiset muokkasivat tukiasemiaan ylimääräisillä signaalinvahvistimilla pidentääkseen niiden kantamaa. Kyseessä oli huomattavasti halvempi ratkaisu saada Internet-yhteys alueille, joissa ei ollut teleoperaattoreiden fyysistä kaapelointia. Pera ymmärsi tässä selvän markkinaraon ja jättäytyikin pian pois Applelta perustaakseen oman yrityksensä. (14; 15.)

3.2 Tuoteperheet

Pera (16) on listannut henkilökohtaisessa blogissaan yrityksen neljä tärkeintä tuotekehityksen suunnitteluperiaatetta:

1. Alkukustannusten tulee olla tarpeeksi alhaisia, jotta jokainen voi ottaa ratkaisun käyttöön.

2. Käyttökokemuksen tulee olla tarpeeksi intuitiivinen, jotta jokainen voi hallinnoida ratkaisua.

3. Suorituskyvyn tulee ylittää operaattoreiden ja yritysten senhetkiset laatuodotukset toiminnollisuuden, suorituskyvyn ja luotettavuuden osalta.

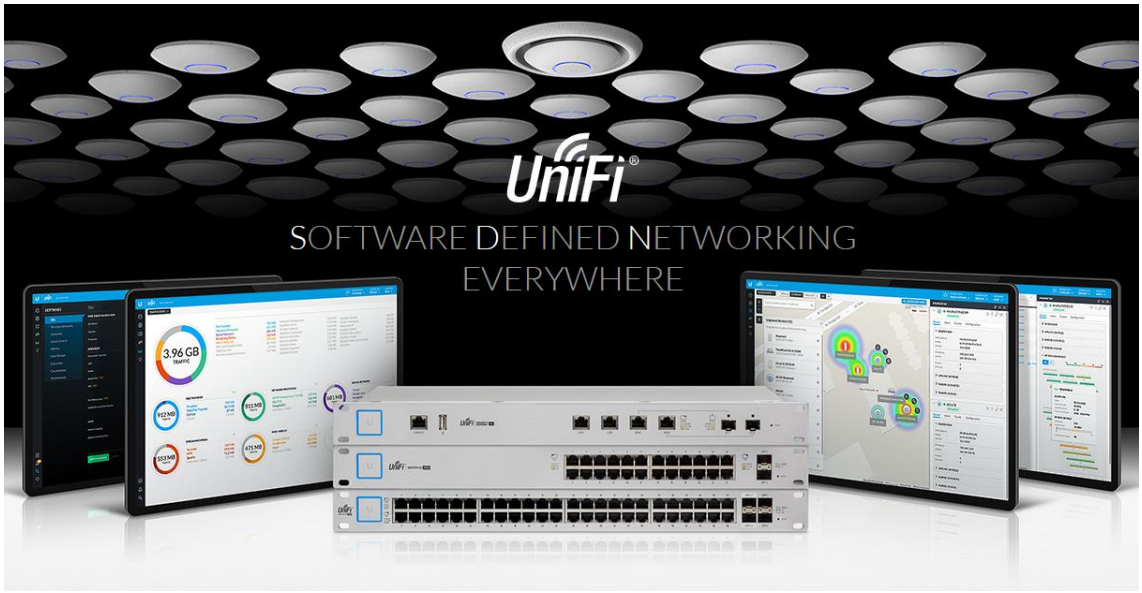
4. Ratkaisun tulee olla tyylikäs – keskittymällä estetiikkaan ja ominaisuuksiin edistetään käyttäjän kiintymystä ja luottamusta.

Panostamalla tuotekehitykseen, luopumalla ylimääräisistä myyntimiehistä ja luottamalla asiakkaiden suusta suuhun -markkinointiin, yritys on onnistunut pitämään käyttökustannukset alhaisina. Uusia ominaisuuksia ja tuotteita ehdotetaan aktiivisesti yrityksen perustaman keskustelupalstan kautta, jossa on yli 1 000 aktiivista käyttäjää päivittäin ja yli miljoona lähetettyä viestiä. Yhteisön edistyneemmät käyttäjät myös testaavat uusimpia käyttöjärjestelmäpäivityksiä. (10.)

Ubiquitilla on laaja valikoima tuotteita eri käyttötarkoituksiin. Langattomiin jakelulinkkeihin keskittyvät tuotteet on sijoitettu airMAX- ja airFiber-tuoteperheisiin. Uutena aluevaltauksena yritys tarjoaa kokonaisvaltaista ratkaisua aurinkoenergian hyödyntämiseen sunMAX-nimen alla. Tässä raportissa keskitytään kuitenkin pääosin EdgeMAX- ja UniFi-tuoteperheisiin. (17.)

EdgeMAX-tuoteperhe koostuu EdgeRouter- ja EdgePoint-reitittimistä sekä EdgeSwitch-kytkimistä. Reitittimiin on asennettuna EdgeOS-käyttöjärjestelmä, jota käsitellään tarkemmin luvussa 3.3. (18.)

UniFi-tuoteperheessä on tavoiteltu helppoa käyttöönottoa ja hallintaa. Pääosin yrityksille markkinoidussa tuoteperheessä on langattomia tukiasemia, reitittimiä, kytkimiä, valvontakameroita ja Android-käyttöjärjestelmän sisältäviä VoIP-puhelimia (Voice over IP) (18). Laitteita hallinnoidaan keskitetysti UniFi Controller -verkonhallintajärjestelmällä, jota käsitellään tarkemmin luvussa 3.4. UniFi-tuoteperhettä markkinoidaan lauseella ” Software Defined Networking Everywhere” (kuva 6).



Kuva 6. ”Software Defined Networking Everywhere” -mainoslause Ubiquitin sivuilla (19).

Seuraavassa on suora lainaus UniFi-VoIP-puhelimien markkinointisivulta, jossa UniFi-kontrolleria nimitetään SDN-ratkaisuksi:

> Ubiquiti’s proprietary SDN software, the UniFi®Controller, provides scalable system management of Android-based UniFi VoIP Phones, including extension management, mass firmware upgrades, and mass configuration provisioning. (20.)

Kuten raportin ensimmäisissä kappaleissa todettiin, SDN-arkkitehtuurin tarkoitus on erottaa ohjauskerros verkkolaitteista. Tutkimalla Ubiquitin tuotteiden ominaisuusselosteita havaitsin, etteivät laitteet tue mitään yleistä SDN-protokollaa kuten OpenFlowta. Yrityksen keskustelupalstalla on julkaistu puolivirallinen, yksittäisen työntekijän antama lausunto EdgeOS-käyttöjärjestelmän OpenFlow-tuesta. Vuonna 2012 julkaistussa viestissä työntekijä kertoo, että OpenFlow-tuen lisäämisestä Ubiquitin laitteille ei ole tarkempia suunnitelmia. (21.)

3.3 EdgeOS-käyttöjärjestelmä

EdgeOS-käyttöjärjestelmä on asennettuna EdgeRouter- ja EdgePoint-reitittimiin (22). Laitteissa käytetään MIPS-arkkitehtuuriin (Microprocessor without Interlocked Pipeline Stages) pohjautuvia prosessoreita (23, s. 6–9; 24, s. 5–6). Luvussa käsitellään EdgeOSin reitityksen ja palomuurin toimintaa, ja esitellään konfigurointiin tarkoitetut käyttöliittymät.

EdgeOS on muunnos Debian GNU/Linuxiin pohjautuvasta avoimen lähdekoodin Vyatta-käyttöjärjestelmästä, tarkemmin ottaen Vyattan versiosta 6.3, joka julkaistiin kesällä 2011. Saman vuoden keväällä osa Vyattan kehittäjistä oli jo siirtynyt Ubiquitille työskentelemään EdgeOSin parissa. Verkko- ja tallennusratkaisuja tarjoava Brocade osti Vyattan vuoden 2012 lopussa, ja sen avoin kehitys lopetettiin. Syksyllä 2013 aloitettiin uusi avoimen lähdekoodin projekti nimeltä VyOS, jonka pohjalla käytettiin Vyattan versiota 6.6. Jos haluaa saada tuntumaa EdgeOS-käyttöjärjestelmän toiminnasta, kannattaa tutustua VyOSiin. (25; 26; 27.)

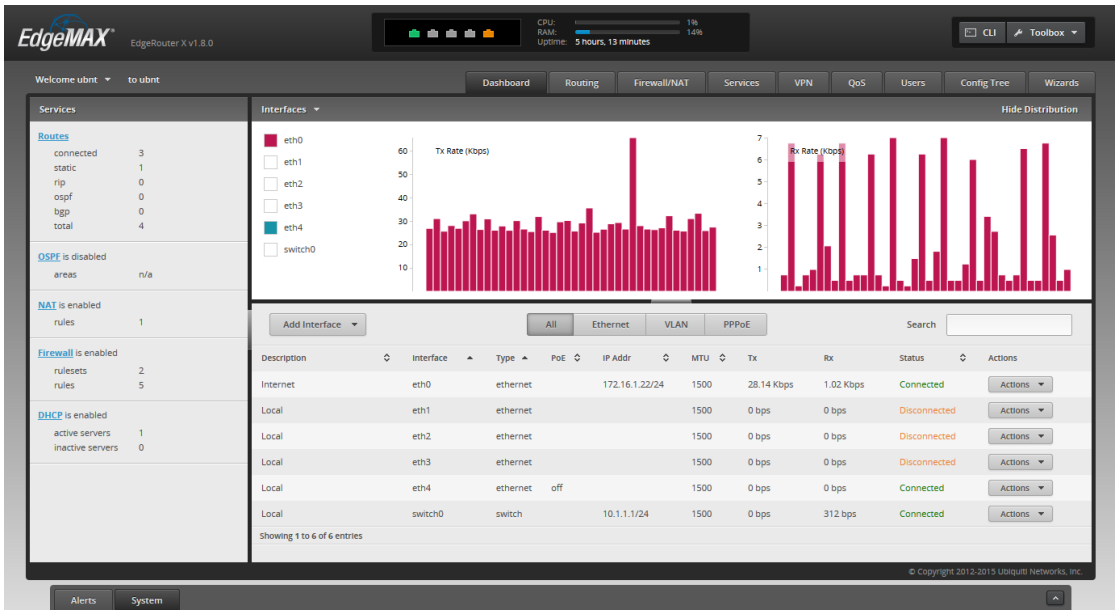
Linux-pohjaisuus tuo käyttöjärjestelmään paljon laajennettavuutta. Järjestelmään on mahdollista asentaa MIPS-arkkitehtuurille käännettyjä Debian-ohjelmistopaketteja, kuten Wake-On-LAN-toiminto, jonka avulla laitteita voidaan herättää lepotilasta verkon välityksellä (28). Ubiquitin verkkosivuilla kehotetaan kuitenkin varovaisuuteen, sillä osa ohjelmistopaketeista on muokattu vain EdgeOS-käyttöjärjestelmän tarpeisiin sopivaksi. Pakettien päivittäminen Debianin komennoilla, kuten apt-get upgrade, saattaa rikkoa järjestelmän toiminnollisuutta. Ohjelmistopakettien tulee olla yhteensopivia myös yleisimpiä UNIX-työkaluja yhdeksi tiedostoksi yhdistävän BusyBoxin kanssa. (29; 30.)

Käyttöjärjestelmässä on monipuolinen tuki eri teknologioille ja protokollille. Tuettuna on IPv4:n (Internet Protocol version 4) lisäksi myös uudempi IPv6 (Internet Protocol version 6). Reitityksessä voidaan käyttää staattisten reittien lisäksi yleisempiä dynaamisia reititysprotokollia, kuten OSPF ja BGP. Käyttöjärjestelmän versiosta 1.8.0 lähtien saatavilla on ollut myös MPLS (Multiprotocol Label Switching). (23, s. 10; 24, s. 7; 31.)

EdgeOSin komentoihin ja konfigurointiohjeisiin liittyvä dokumentaatio oli insinöörityön tekoaikaan vielä jonkin verran puutteellista. Ubiquitin sivuilla on käyttöjärjestelmän käyttöopas, mutta siinä käydään läpi pääasiassa vain web-käyttöliittymän ominaisuuksia eikä esimerkiksi palomuurin tai komentorivikomentojen syvällisempää toimintaa. EdgeOS on kehittynyt monella tapaa omaan suuntaansa, mutta Vyattan 6.3 versiota varten kirjoitettu dokumentaatio on edelleen tärkeä tietolähde. Raportissa hyödynnetään Vyattan dokumentaatiota, joka oli kirjoittamisen aikaan saatavilla osoitteessa https://dl.networklinx.com/vyatta/6.3/.

Web-käyttöliittymä

EdgeOS tarjoaa monipuolisen ja intuitiivisen web-käyttöliittymän, jonka kautta pystyy konfiguroimaan suurimman osan järjestelmän toiminnollisuudesta. Käyttöliittymän etusivun päänäkymästä (kuva 7) nähdään tärkeimmät tiedot verkon tilasta. Listattuna on muun muassa staattisten ja dynaamisten reittien määrä. Nähtävissä on myös reaaliaikainen verkkoliikenteen määrä liitäntäkohtaisesti.



Kuva 7. EdgeOS-käyttöjärjestelmän web-käyttöliittymän päänäkymä.

Käyttöjärjestelmässä voidaan käyttää kahta käyttäjäroolia. Admin-tason käyttäjät voivat tehdä muutoksia laitteen konfiguraatioon, jota operator-tason käyttäjät voivat vaan tarkastella. (22, s. 59.)

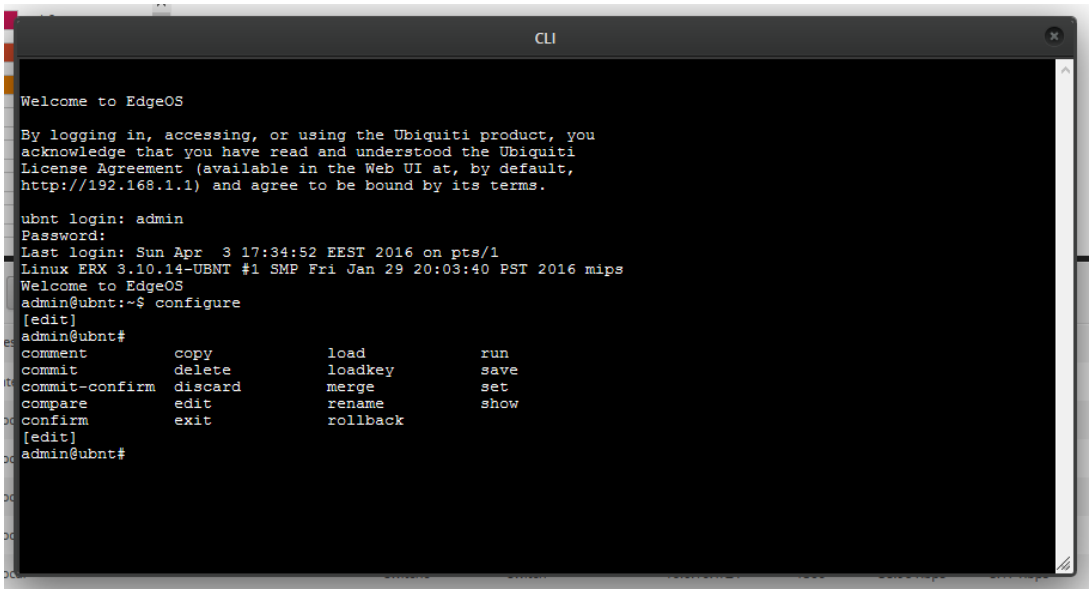
Kaikki oikeudet käyttöjärjestelmään omistaa root-käyttäjä, jolle ei oletuksena ole määritelty salasanaa, mikä estää sen käyttämisen kirjautumiseen. Käyttöjärjestelmään tulee ensin olla kirjautuneena admin-tason käyttäjänä, minkä jälkeen voidaan komentoriviliittymän kautta kirjautua root-käyttäjänä sudo su -komennolla. Sudo-komennolla voidaan tavallisen ylläpitäjän oikeuksia tilapäisesti nostaa pääkäyttäjän tasolle, mikä riittää useimmissa tapauksissa eikä salasanaa pääkäyttäjälle tarvitse määritellä. (32.)

Komentoriviliittymä

Komentoriviliittymä on tekstipohjainen käyttöliittymä, jonka avulla voidaan nopeasti suorittaa monimutkaisiakin toimenpiteitä käyttämällä erilaisia komentoja. EdgeOSin komentoriviliittymä muistuttaa Juniperin Junos-käyttöjärjestelmää (33). Komentoriviliittymään on pääsy web-käyttöliittymän, SSH:n (Secure Shell) tai Telnetin kautta. Telnet on oletusarvoisesti kytketty pois päältä, eikä sen käyttöä suositella, koska se lähettää kirjautumiseen käytetyt tiedot salaamattomana. (22, s. 45–46; 34.)

Komentoriviliittymässä on kaksi tilaa: toiminnallinen (operational mode) ja konfigurointitila (configuration mode). Kirjautumiseen käytetään samoja käyttäjätunnuksia kuin web-käyttöliittymässä. Kirjautumisen jälkeen ollaan suoraan toiminnallisessa tilassa, jonka ilmaisee ~$-merkit käyttäjänimen perässä. Konfigurointitilaan siirrytään configure-komennolla, jonka jälkeen käyttäjänimen perään vaihtuu #-merkki. Käytettävissä olevat komennot saa näkyviin molemmissa tiloissa kirjoittamalla kysymysmerkin (?) komentoriville tai painamalla tabulaattoria näppäimistössä, jolla komentoja voidaan myös automaattisesti täydentää. (22, s. 85.)

Kuvassa 8 on kirjauduttu sisään web-käyttöliittymän kautta avatun komentoriviliittymän kautta, siirrytty konfigurointitilaan ja listattu saatavilla olevat komennot tabulaattorilla. Käytännön toteutusta tehdessäni huomasin, että kysymysmerkin käyttö ei toiminut web-pohjaisessa komentoriviliittymässä, ja sen käyttökokemus oli muutenkin tökkivä.



Kuva 8. EdgeOS-käyttöjärjestelmän web-pohjainen komentoriviliittymä.

Tehtäessä muutoksia konfiguraatioon komentorivin kautta on otettava huomioon, että konfiguraatiosta on samaan aikaan olemassa kolme eri versiota:

- *Boot-konfiguraatiotiedosto* sisältää tallennetun konfiguraation. Tiedosto sijaitsee käyttöjärjestelmän juurihakemistossa /config/config.boot, ja se ladataan laitteen muistiin käynnistyksen yhteydessä.

- *Active-konfiguraatioksi* nimitetään muistiin ladattua kopiota config.boot-tiedostosta.

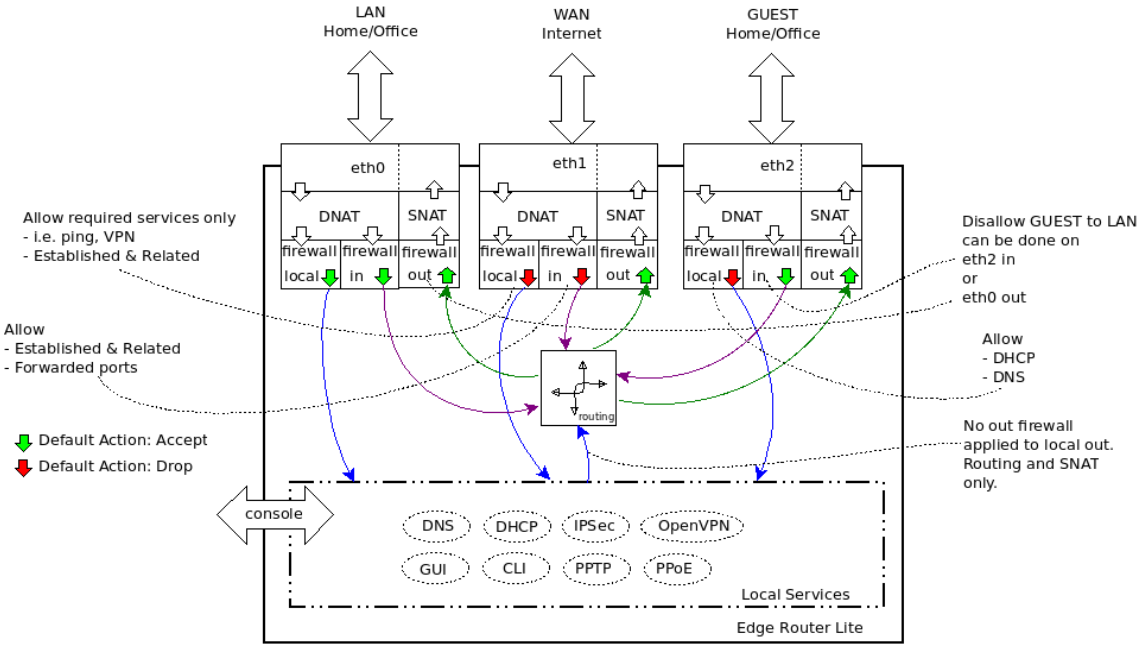
- *Working-konfiguraatioon* tallentuvat komentorivin kautta tehdyt muutokset. Muutokset tulee ottaa käyttöön ja hyväksyä osaksi active-konfiguraatiota suorittamalla commit-komento. Active-konfiguraatioon tehdyt muutokset häviävät, jos laite käynnistetään uudelleen. Muutokset tulee tallentaa config.boot-tiedostoon suorittamalla save-komento. (22, s. 86.)

Konfiguraation muokkauksessa tärkeitä komentoja ovat show, set, edit, delete, compare ja discard. Show-komento näyttää nykyisen arvon, esimerkiksi liitännän IP-osoitteen. Set-komennolla muutetaan tai asetetaan arvo. Edit-komennolla voidaan muokata suurempia kokonaisuuksia kerralla. Delete-komento poistaa arvoja. Compare-komento näyttää Working-konfiguraatioon tehdyt muutokset, jotka otetaan käyttöön commit-komennon jälkeen. Discard-komento hävittää tehdyt muutokset. (22, s. 85–87.)

Palomuuri

Käyttöjärjestelmässä on mahdollista käyttää pääsylistapohjaista (ACL-based) ja vyöhykepohjaista (Zone-based) palomuuria (23, s. 10; 24, s. 7). Vyöhykepohjainen palomuuri on toistaiseksi konfiguroitavissa ainoastaan komentorivin kautta (35). Palomuurin toiminta ja yksittäiset komentorivikomennot ovat edelleen parhaiten kuvattuna Vyattan palomuuria käsittelevässä dokumentaatiossa (36).

Pääsylistapohjaisessa palomuurissa käyttäjän määrittelemät palomuurisäännöt lisätään johonkin reitittimen liitäntään, kuten eth0, avainsanalla in, out tai local. Reitittimelle saapuva paketti voidaan estää (drop) ennen reitityksen tapahtumista (in), mikä on suositeltavaa, tai vasta reitityksen jälkeen (out), kun paketti on poistumassa jostain reitittimen toisesta liitännästä. Avainsanalla local tarkoitetaan reitittimen paikallisia palveluja, kuten web-käyttöliittymää. Internetistä saapuva verkkoliikenne on siis hyvä olla suodatettu in ja local avainsanoilla. Tällä tavalla ulkopuolelta ei ole pääsyä reitittimen web-käyttöliittymään tai sisäverkkoon. Liikenteen virtausta pääsylistapohjaisen palomuurin läpi havainnollistaa EdgeRouter Lite -reitittimelle tarkoitettu ohjeellinen kuva 9. Kaikki reitittimen liitännät toimivat samalla periaatteella. (36, s. 2–3.)

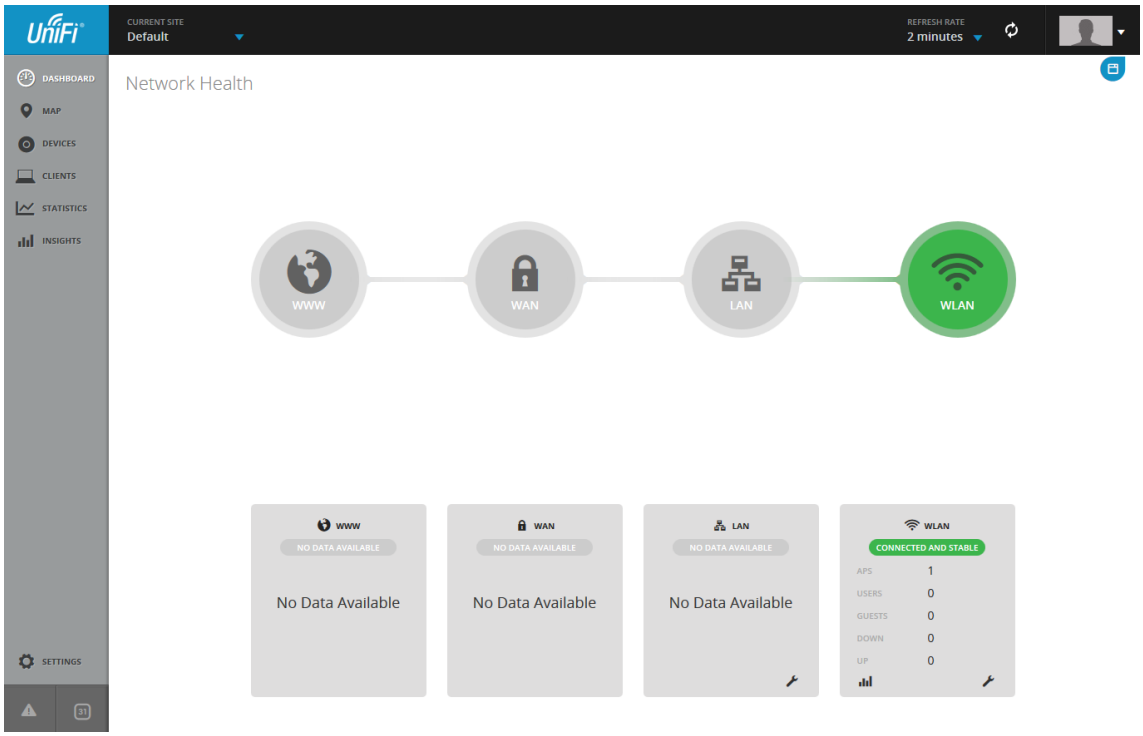


Kuva 9. Liikenteen virtaus palomuurin läpi ja reitityksen rooli (37).

3.4 UniFi Controller -verkonhallintajärjestelmä

UniFi-tuoteperheen laitteiden hallinnointiin, lukuun ottamatta valvontakameroita, käytetään UniFi Controlleria, joka voidaan asentaa Windows-, Mac OS X- ja Linux-käyttöjärjestelmään (38, s. 1). Kontrolleri on ladattavissa ilmaiseksi Ubiquitin verkkosivuilta osoitteesta https://www.ubnt.com/download/unifi. Osaan kontrollerin ominaisuuksista voi tutustua omistamatta yhtään UniFi-laitetta.

Kontrolleri on ohjelmoitu Java-kielellä, joten sen suorittamisen tarvitaan Java Runtime Environment 1.6 tai uudempi (38, s. 1). Kontrolleria konfiguroidaan pääasiassa web-käyttöliittymän kautta, jonka etusivulla olevasta Network Health -näkymästä nähdään verkon senhetkinen tila (kuva 10). WWW- (World Wide Web), WAN- ja LAN-symbolit ovat käytössä, jos hallinnoitavassa verkossa sijaitsee UniFi Security Gateway -reititin ja UniFi Switch -kytkmiä. WLAN-symboli viittaa UniFi-tukiasemiin. Vihreä väri tarkoittaa, että laite tai laitteet ovat aktiivisia ja saatavilla. Punainen ilmaisee, että laitteisiin ei saada yhteyttä tai ne ovat pois päältä. Harmaa kertoo, että kyseisen kategorian laitteita ei sijaitse tässä verkossa. (38 s. 34.)



Kuva 10. UniFi-kontrollerin web-käyttöliittymän Network Health -näkymä versiossa 4.8.15.

Kontrollerissa voidaan konfiguroida useita erillisiä verkkokokonaisuuksia (site), joista jokaiseen kuuluu omat laitteet, konfiguraatio, pohjakartat ja käyttöstatistiikka (38 s. 18). Näin yrityksen haarakonttoreiden laitteita voidaan hallinnoida samalla, esimerkiksi pilvipalveluun sijoitetulla kontrollerilla. Hallintaliittymään on mahdollista ladata rakennusten ja huoneiden pohjakarttakuvia, johon laitteista voidaan sijoittaa kuvakkeet vastaamaan niiden fyysistä sijaintia. Tämä selkeyttää ylläpitoa, sillä kuvakkeen kautta on suora pääsy laitteen asetuksiin. Pohjakartalle on myös mahdollista määrittää mittasuhteet, jolloin sen avulla voidaan simuloida tukiasemien yhteyden kantamaa. (38, s. 32.)

Hallintaliikenne

Luvussa 2.1.4 esiteltiin yhdeksi ohjelmisto-ohjattujen ominaisuudeksi, että ne tukevat OpenFlowta tai jotain muuta SDN-protokollaa. UniFi-tuoteperheessä kontrollerin ja laitteiden välinen hallintaliikenne on toteutettu SSH-yhteydellä.

Hallintaliikenne kulkee ilman VLAN-tunnistetta (untagged), mikä mahdollistaa kontrollerin sijoittamisen esimerkiksi pilvipalveluun. Hallinnoitava laite noutaa IP-osoitteen dynaamisesti oman aliverkkonsa DHCP (Dynamic Host Configuration Protocol) -palvelimelta ja alkaa lähettää majakkaviestiä (beacon) yleislähetyksenä (broadcast) verkon siirtokerroksessa. Kontrollerin kuultua majakkaviestin laite ilmestyy hallintapaneeliin, minkä jälkeen se voidaan liittää kontrolleriin. Kontrolleri suorittaa liittämisprosessin kirjautumalla tukiasemaan SSH-yhteydellä käyttäen oletuskäyttäjätunnuksia ja lisää oman IP-osoitteensa tukiaseman asetuksiin.

Laite lähettää tiedon onnistuneesta liittämisestä kontrollerille. Liittämisen jälkeen laite säännöllisesti ”soittaa kotiin” eli pyytää kontrollerilta suoritettavia toimenpiteitä. Asetuksia pystytään myös ”puskemaan” laitteille tarvittaessa. Jos yhteys kontrolleriin jostain syystä katkeaa, laite alkaa lähettää majakkaviestiä uudelleen. Kun yhteys kontrolleriin on palautunut, laite otetaan automaattisesti uudelleen hallintaan SSH-yhteydellä. (39.)

Hallintaliikenteen toteutustavasta voidaan todeta, että se on lähempänä WLAN-kontrolleria tai jonkinlaista verkonhallintajärjestelmää kuin ohjelmisto-ohjattua verkkoratkaisua.

4 Testiympäristön toteuttaminen

4.1 Alkuasetelma

Olin jo pitkään pohtinut oman kotiverkkoni reitittimen korvaamista jollakin tehokkaammalla ja monipuolisemmalla vaihtoehdolla. Opiskelukaverini olivat hankkineet Ubiquitin reitittimiä ja tukiasemia. Heidän suosittelujensa perusteella päädyin itsekin hankkimaan EdgeRouter Lite -reitittimen, mutta en vielä siinä vaiheessa ollut päättänyt tehdä aiheesta insinöörityötä. Tutustuessani tarkemmin laitteen toimintaan sain idean myös dokumentoida tämän prosessin. En löytänyt kattavaa aiempaa tutkimusta Ubiquitista tai sen tuotteista, joten päädyin tekemään insinöörityön aiheesta.

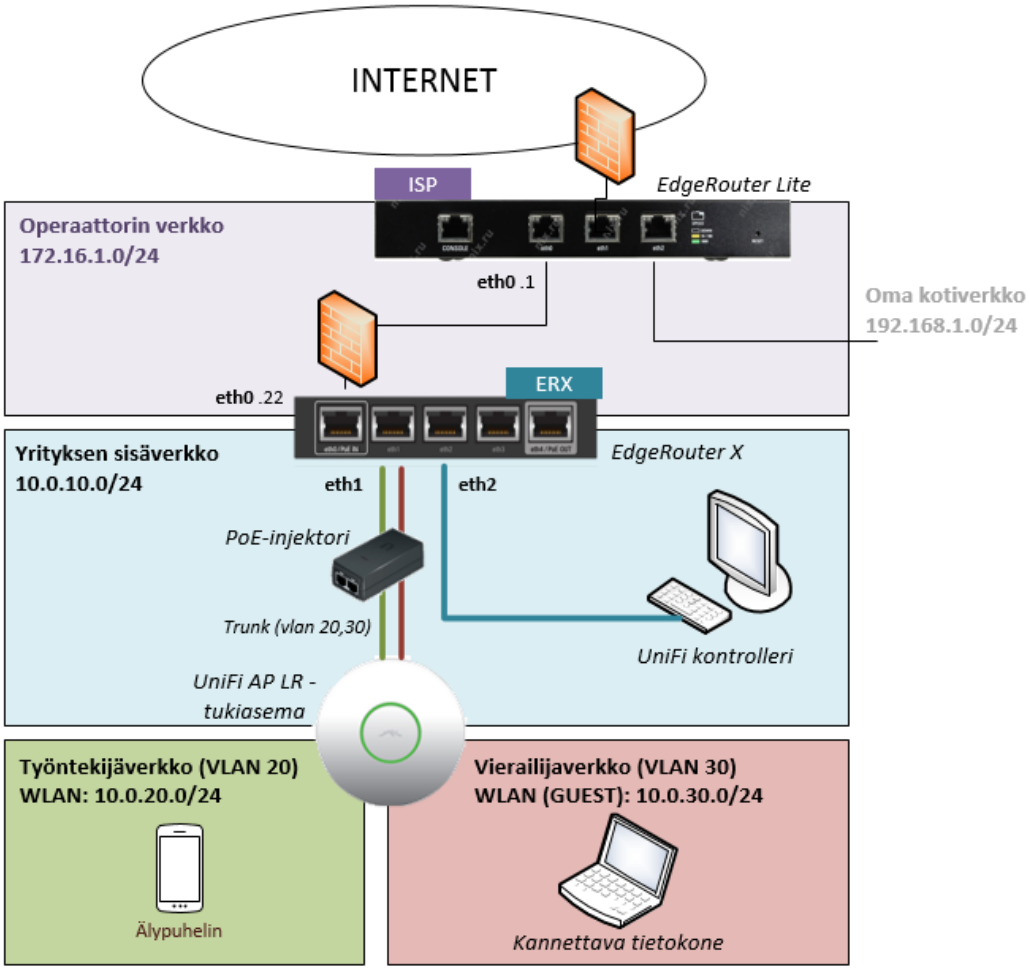
Aloin etsiä maahantuojia, jotka voisivat lainata Ubiquitin tuotteita testaukseen. Otin yhteyttä pietarsaarelaiseen Noyra Oy:hyn, joka myy Ubiquitin laitteiden lisäksi myös konsultointipalveluita Suomessa. Aluksi pyysin testiin uusimpia UniFi AC Pro -tukiasemia, mutta näitä ei vielä työn aloittamisen aikaan ollut helposti saatavilla. Yritys tarjoutui kuitenkin lainaamaan seuraavat tuotteet testattavaksi: EdgeRouter X -reitittimen, UniFi AP LR -tukiaseman, UniFi Video Camera Micro -valvontakameran ja airMAX-tuoteperheeseen kuuluvan Nanostation Loco 2 -tukiaseman.

4.2 Määrittely

Aluksi tutustuin laitteiden hallintaliittymään ja ominaisuuksiin yleisellä tasolla, minkä jälkeen testasin valvontakameraa ja sen hallinnointiin tarkoitettua UniFi Video -hallintaohjelmistoa. Lopulta päätin ottaa tarkempaan analyysiin EdgeRouter X -reitittimen ja UniFi AP LR -tukiaseman, ja rakentaa omaan kotiverkkooni testiympäristön, johon kuuluisi kuvitteellinen operaattorin verkko ja yrityksen verkko. Oma EdgeRouter Lite -reitittimeni, josta jatkossa käytän nimitystä ISP (Internet Service Provider), on kuvitteellisen operaattoriverkon reititin, joka jakaa IP-osoitteita DCHP:n avulla. ISP:n kautta on pääsy myös Internetiin. EdgeRouter X toimii kuvitteellisen yrityksen reunareitittimenä, ja siitä käytetään jatkossa nimitystä ERX. Yrityksen langaton verkko toteutetaan UniFi AP LR -tukiasemalla.

Työntekijöille tarkoitetun langallisen ja langattoman verkon lisäksi luodaan erillinen vierailijaverkko. Vierailijaverkko eristetään verkkokerroksella ja siirtokerroksella muusta sisäverkosta. Vierailijaverkolle määritellään latausnopeudeksi 2 Mb/s ja lähetysnopeudeksi 1 Mb/s.

Selventääkseni toteutusta käytän useaa yksityisille lähiverkoille varattua IP-osoiteavaruutta erottamaan verkon osat toisistaan (kuva 11). Oman kotiverkkoni osoiteavaruus on 192.168.0.0/16, joten operaattoriverkolle määrittelin 172.16.1.0/24. Yrityksen sisäverkossa on käytössä 10.0.0.0/8-osoiteavaruus, josta 10.0.10.0/24 on varattu langalliselle verkolle, 10.0.20.0/24 langattomalle työntekijäverkolle ja 10.0.30.0/24 langattomalle vierailijaverkolle. Kontrolleri, jolla tukiaseman asetukset ja muu konfigurointi tehdään, on kytketty yrityksen langalliseen verkkoon.



Kuva 11. Testiympäristön verkkotopologia.

4.3 EdgeRouter X -reitittimen käyttöönotto

EdgeRouter X (kuva 12) on tehokas ja pienikokoinen reititin, jolla on hyvä hinta-laatusuhde. Laite julkaistiin huhtikuussa 2015, ja se on tällä hetkellä EdgeMAX-tuoteperheen edullisin reititin (40). Sen hinta Ubiquitin omassa verkkokaupassa, joka on tarkoitettu vain Yhdysvalloissa asuville asiakkaille, on 49 dollaria (41).

Kuva 12. EdgeRouter X:n etupaneeli.

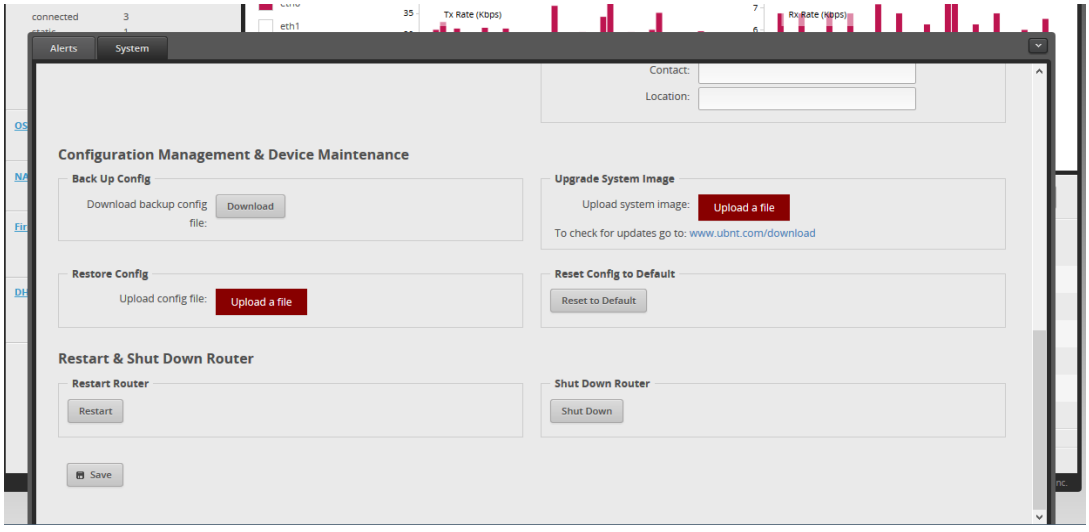
EdgeRouter X:n tärkeimmät tekniset ominaisuudet:

- mitat 110 x 75 x 22 mm (leveys, syvyys, korkeus)
- paino 175 g
- virrankulutus korkeintaan 5 W
- 880 MHz MIPS1004Kc -kaksiydinprosessori
- 256 MB DDR3 RAM-muistia
- 256 MB:n NAND-siru
- viisi 10/100/1000 nopeuksista RJ45-liitäntää:
    - kolme tavallista RJ45-liitäntää (eth1, eth2, eth3)
    - yksi RJ45-liitäntä, jossa PoE-virran sisääntulo (eth0)
    - yksi RJ45-liitäntä, jossa PoE-virran ulostulo (eth4) (24, s. 5).

Käyttöjärjestelmän päivitys

Reitittimeen on oletuksena konfiguroitu IP-osoite 192.168.1.1 eth0-liitäntään. Palomuuri ja DHCP-palvelin ovat kytketty pois päältä. Määritin reitittimen konfigurointiin käytettävälle tietokoneelle staattisen IP-osoitteen 192.168.1.0/24 aliverkosta ja kirjauduin reitittimen web-käyttöliittymään. Ensimmäisenä päätin asentaa reitittimeen uusimman firmware-päivityksen, joka raportin kirjoittamisen aikaan oli helmikuussa 2016 julkaistu versio 1.8.0 (22). Päivitykset sisältävät uusia ominaisuuksia, ohjelmistovirhekorjauksia ja tietoturvaparannuksia, joten ne on suositeltavaa asentaa. Ennen päivittämistä kannattaa kuitenkin tutustua huolellisesti kyseisessä päivityksessä tehtyihin muutoksiin ja muilla käyttäjillä mahdollisesti ilmenneisiin ongelmiin. Käyttöjärjestelmän versiossa 1.8.0 esimerkiksi osa BGP-reititysprotokollan konfigurointiin tarkoitetuista komennoista poistettiin käytöstä (42). Vanhentuneita komentoja käyttävät konfiguraatiot eivät siis enää toimisi päivityksen jälkeen.

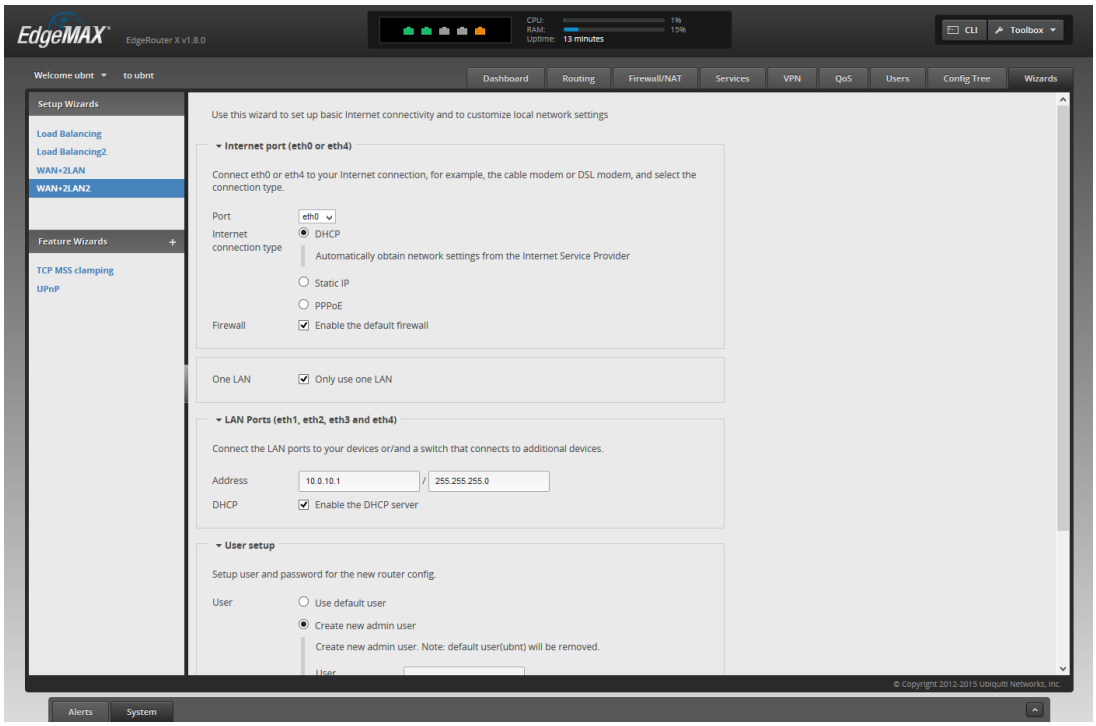
EdgeRouterin eri malleille on olemassa mallikohtaiset firmware-päivityspaketit. Päivittäminen voidaan suorittaa joko web-käyttöliittymän tai komentorivin kautta (43). Käytin itse web-käyttöliittymään sen helppouden takia. Päivitys suoritetaan web-käyttöliittymän järjestelmäasetuksista, jonne pääsee selainikkunan alareunassa sijaitsevalla System-painikkeella. Järjestelmäasetuksissa on Upgrade System Image -kohta, josta päivityspaketti asennetaan reitittimeen (kuva 13).



Kuva 13. Reitittimen järjestelmäasetukset web-käyttöliittymässä.

Nopea konfigurointi käyttöönottoapurilla

Yhtenä tutkimuskohteena oli selvittää laitteiden helppoa käyttöönottoa. EdgeOSissa on tähän tarkoitukseen muutamia valmiita käyttöönottoapureita. Testasin WAN+2LAN2-käyttöönottoapuria (kuva 14), ja selvitin tarkemmin sen tekemiä määrittelyjä.



Kuva 14. WAN+2LAN2-käyttöönottoapuri EdgeOS-käyttöjärjestelmän versiossa 1.8.0.

Liitännäksi, joka määritellään olevan yhteydessä Internetiin, voidaan valita käyttöönottoapurin kautta joko eth0 tai eth4. Jätin eth0-liitännän valituksi, koska haluan säilyttää mahdollisuuden tulevaisuudessa liittää PoE-laitteen eth4-liitäntään, josta kerrotaan raportissa myöhemmin, ilman konfiguraatiomuutoksia.

Laajakaistaliittymissä ei yleensä ole staattista ulkoista IP-osoitetta, vaan osoite noudetaan DHCP:n avulla palveluntarjoajalta. Tämä on myös käyttöönottoapurissa oletusarvoinen IP-osoitteen määritystapa ja jätin sen valituksi, koska IP-osoite noudetaan ISP:ltä. Osoitteenmuunnos eli NAT (Network Address Translation) otetaan automaattisesti käyttöön kyseiselle liitännälle. Osoitteenmuunnoksen avulla sisäverkon laitteet voivat kommunikoida Internetiin yhden palveluntarjoajalta saadun ulkoisen IP-osoitteen kautta. (22, s. 72.)

Enable the default firewall -toiminto ottaa käyttöön palomuurisäännöt Internetiin kytketylle liitännälle. Säännöt sallivat vain sisäverkosta päin muodostettujen yhteyksien muodostuksen ja jatkumisen (22, s. 73). Internetistä tulevat kyselyt eivät saa aikaan mitään vastausta reitittimeltä, mutta sisäverkon päätelaitteelta tehty verkkoselailu onnistuu ongelmitta.

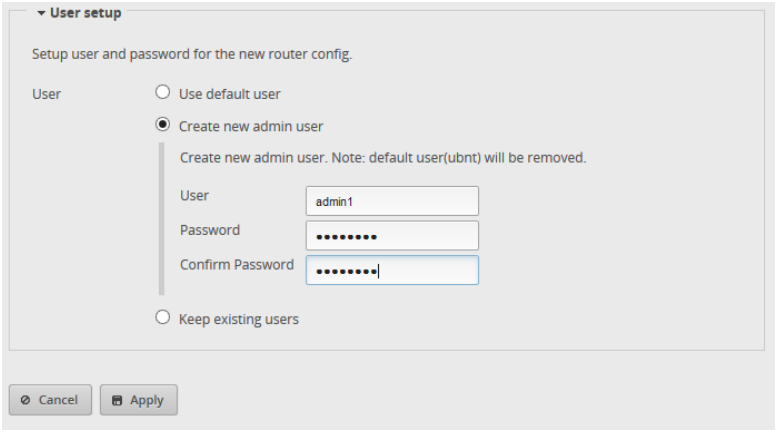
Käyttöönottoapuri luo kaksi pääsylistaa, WAN_IN ja WAN_LOCAL, jotka poikkeavat toisistaan vain nimeltään ja kuvaukseltaan, mutta ovat muuten määrityksiltään samanlaiset. Palomuurisääntöjen konfiguraatio esitetään komentorivimuodossa tiiviimmän esitystavan vuoksi. Tarkemmat määrittelyt ovat nähtävissä liitteestä 1.

```
name WAN_IN {
    default-action drop
    description "WAN to internal"
    rule 10 {
        action accept
        description "Allow established/related"
        state {
            established enable
            related enable
        }
    }
    rule 20 {
        action drop
        description "Drop invalid state"
        state {
            invalid enable
        }
    }
}
```

Käyttöönottoapuri lisää pääsylistat liitäntään, joka on kytketty Internetiin, avainsanoilla in ja local, joten näin paketit käsitellään niiden tullessa sisään liitännästä ja reitititintä kohden. Internetiin kytketyn eth1-liitännän käyttöönottoapurin tekemät määrittelyt ovat seuraavanlaiset:

```
ethernet eth1 {
    address dhcp
    description Internet
    duplex auto
    firewall {
        in {
            name WAN_IN
        }
        local {
            name WAN_LOCAL
        }
    }
}
```

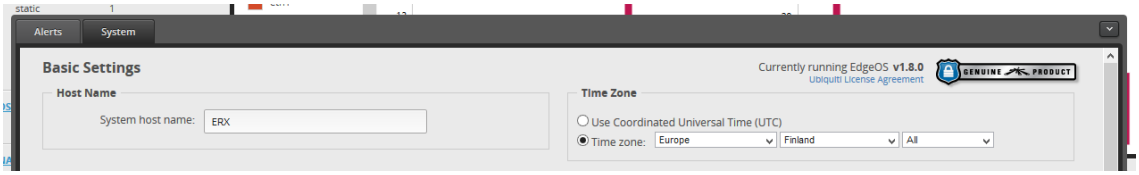
EdgeRouter X -mallissa on ohjelmistopohjainen Switch0-liitäntä, jonka avulla laitteen fyysiset liitännät voidaan määrittää toimimaan kytkinporttien tapaan. Valitsemalla käyttöönottoapurista *Only use one LAN* -valintaruutu, voidaan eth1-eth4-liitännät muuttaa kytkinporteiksi, jotka määrittelin kaikki sijaitsemaan verkossa 10.0.10.0/24. Tutkimuksissa selvisi, että *Enable the DHCP server* -asetus luo aliverkolle DHCP-palvelimen jakamaan IP-osoitteita osoitealueesta, jonka ensimmäinen osoite on 10.0.10.38 ja viimeinen 10.0.10.243. Käyttöjärjestelmän versiossa 1.8.0 käyttöönottoapuriin lisättiin ominaisuus korvata reitittimen oletuskäyttäjä ubnt jollain muulla (31). Aiemmin uuden käyttäjätunnuksen luominen ja oletuskäyttäjän poistaminen tuli suorittaa manuaalisesti. Käyttöönottoapurin *User setup* -kohdassa luodaan uusi admin-tason käyttäjä keskivahvalla salasanalla (kuva 15).



Kuva 15. Uuden käyttäjätunnuksen luominen WAN+2LAN2-käyttöönottoapurin avulla.

Käyttöönottoapurin avulla tehdyt muutokset otetaan lopuksi käyttöön Apply-painikkeella, ja reititin käynnistyy uudelleen. Tämän jälkeen reitittimeen on konfiguroitu yksinkertainen mutta peruskäyttöön tarpeeksi riittävä palomuuri, ja se pystyy reitittämään liikennettä sisäverkon ja ulkoverkon välillä. Liitteestä 1 on nähtävissä tarkemmin kaikki käyttöönottoapurin tekemät määrittelyt. Määrittelyjen konfiguroiminen käsin veisi huomattavan paljon aikaa.

Isäntänimen asettaminen helpottaa laitteen tunnistettavuutta sisäverkossa, ja oikean aikavyöhykkeen määrittäminen on erityisen tärkeää, jotta reitittimen lokitiedostoihin tallentuu tapahtumien oikea aikaleima. Asetin isäntänimeksi ERX ja aikavyöhykkeeksi Europe/Finland web-käyttöliittymän järjestelmäasetuksista (kuva 16).



Kuva 16. Isäntänimi ja aikavyöhyke voidaan asettaa web-käyttöliittymän järjestelmäasetuksista.

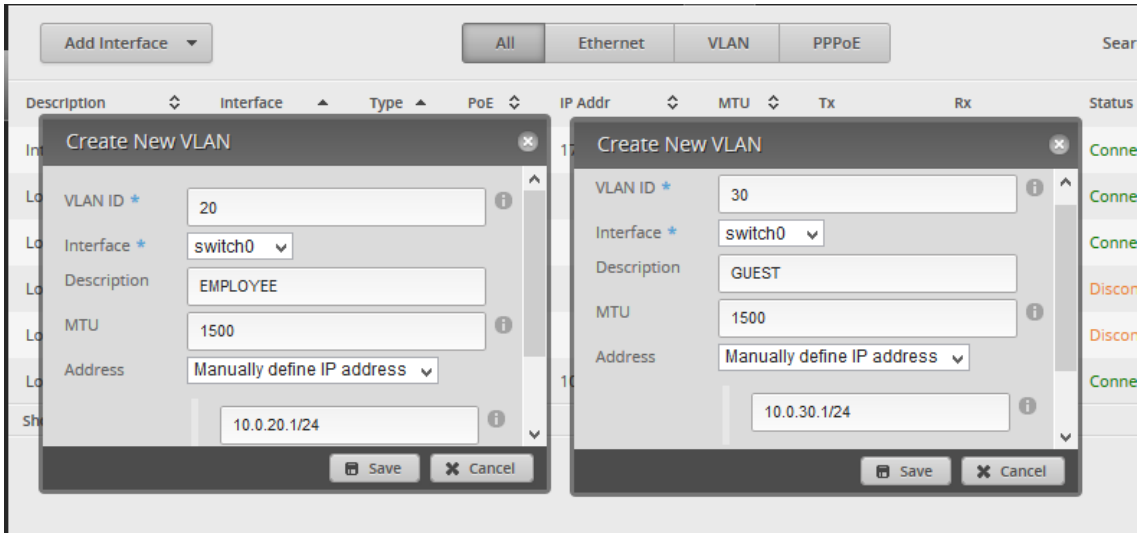
Virtuaalisten lähiverkkojen luominen

Virtuaalisten lähiverkkojen (VLAN) konfiguroiminen mahdollistaa verkon segmentoimisen ja tarvittaessa liikenteen rajoittamisen. Loogisella IP-osoitteiden määrityksellä nähdään myös helposti päätelaitteiden liityntäpiste verkkoon. Osoitteesta 10.0.20.102 tiedetään heti sen olevan liitettynä langattomaan työntekijäverkkoon. Tästä on hyötyä verkon valvonnassa.

VLANien toteuttaminen loi hieman haasteita, koska käytössä ei ollut kytkintä. EdgeRouter X:ssä on mahdollisuus liittää VLANit joko tavalliseen eth-liitäntään tai switch0-liitäntään, joka siis pystyy yhdistämään useamman eth-liitännän. Näin VLANit ovat oletuksena saavutettavissa verkon siirtokerroksessa joko yhdestä eth-liitännästä tai kaikista switch0-liitäntään yhdistetyistä eth-liitännöistä. Päätin joka tapauksessa konfiguroida VLANit switch0-liitäntään, koska näin UniFi-tukiasema saa IP-osoitteen 10.0.10.0/24 aliverkosta, ja kontrollerin on helpompaa automaattisesti tunnistaa se samassa levitysviestialueessa (39). Kyseessä on kuitenkin reititin, joka pystyy automaattisesti reitittämään VLANien välillä, kunhan niiden oletusyhdyskäytävällä on IP-osoite. DHCP-

palvelin on mahdollista konfiguroida mainostamaan kontrollerin IP-osoitetta oman aliverkkonsa päätelaitteille *DHCP Option 43* -toiminnolla (kuva 18) (38, s. 123–124). Jos laite on UniFi-tukiasema, saa se näin tietää kontrollerin sijainnin verkossa. (22, s. 40.)

Langattomalle työntekijäverkolle luodaan päänäkymästä *Add Interface* -painikkeella VLAN tunnistenumerolla 20, ja asetetaan sen IP-osoitteeksi ensimmäinen osoite 10.0.20.0/24 aliverkosta (kuva 17). Kuvaukseksi määritellään EMPLOYEE. Vierailijaverkolle luodaan VLAN tunnistenumerolla 30 ja kuvauksella GUEST. Vierailijaverkon VLAN-liitännän IP-osoitteeksi määritellään ensimmäinen osoite 10.0.30.0/24 aliverkosta.

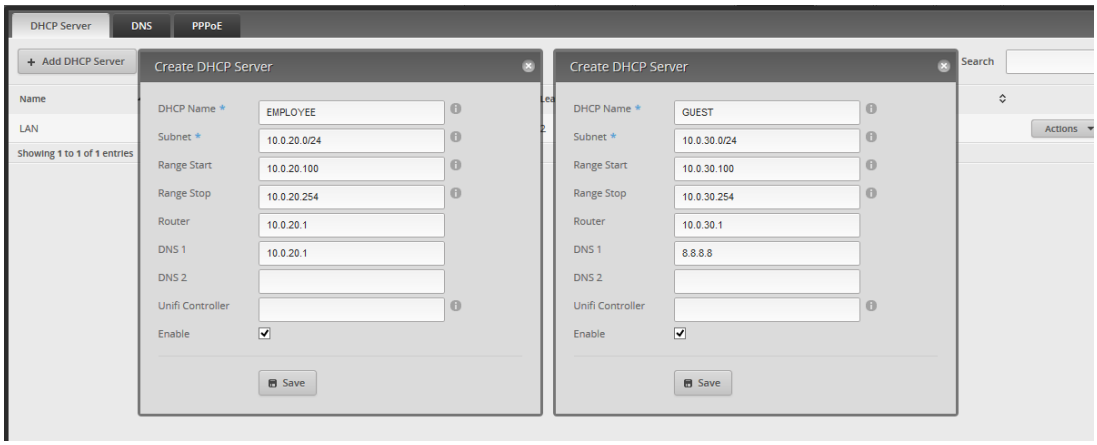


Kuva 17. VLANien luominen web-käyttöliittymällä.

DHCP-osoitealueet

DHCP-osoitealueet luodaan web-käyttöliittymän palvelut (Services) -sivun kautta siten, että osoitealue alkaa osoitteesta 10.0.X.100, jossa X vastaa VLAN-tunnistetta, ja päättyy osoitteeseen 10.0.X.254. Työntekijäverkolle tarkoitettu osoitealue luodaan nimellä EMPLOYEE. Oletusyhdyskäytäväksi ja nimipalvelimeksi asetetaan VLANin IP-osoite 10.0.X.1. DHCP:n jakamien IP-osoitteiden laina-ajaksi tulee automaattisesti 86 400 sekuntia eli 24 tuntia, mikä on mielestäni sopiva laina-aika päätelaitteille. Vierailijaverkolle tämä voisi olla lyhyempi. Arvoa pystyy muuttamaan DHCP-palvelimen luomisen jälkeen. Vierailijaverkon DHCP-osoitealue luodaan nimellä GUEST, mutta muuten samoilla periaatteilla kuin työntekijäverkon DHCP-palvelinkin. Reitittimestä halutaan pal-

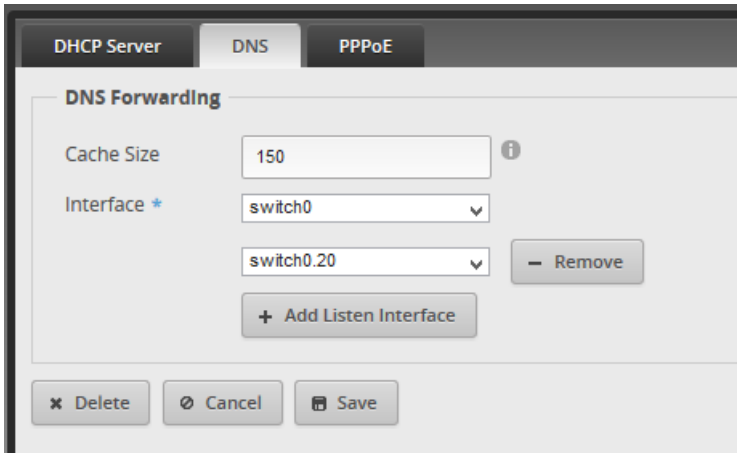
jastaa vierailijaverkolle mahdollisimman vähän. Tästä syystä vierailijaverkolle asetetaan Googlen tarjoama nimipalvelin, jonka IP-osoite on 8.8.8.8. Määrittelyt nähdään tarkemmin kuvasta 18. Muutin myös langallisen verkon noudattamaa samaa osoitealueen määrittelyä kuin langattomilla verkoilla. Reititin käyttää automaattisesti oikeaa DCHP-palvelinta jakamaan osoitteita aliverkkojen päätelaitteille.



Kuva 18. DHCP-palvelimien luonti web-käyttöliittymästä.

DNS-ohjaus

Käyttöönottoapuri teki automaattisesti langalliselle verkolle DNS-ohjauksen, mutta työntekijäverkolle se tulee asettaa käsin palveluiden DNS-välilehdestä. Lisäsin uuden DNS-ohjauksen *Add Listen Interface* -painikkeella liitännälle switch0.20, joka siis viittaa työntekijäverkolle luotuun VLAN-liitäntään (kuva 19).



Kuva 19. DNS-ohjauksen luominen web-käyttöliittymästä.

4.4 UniFi AP LR -tukiaseman käyttöönotto

Langaton verkko toteutetaan UniFi AP LR -tukiasemalla (kuva 20), joka tukee muun muassa IEEE 802.11n -standardia (44, s. 12). Tukiaseman hinta Ubiquitin omassa verkkokaupassa on 89 dollaria (45). Markkinoille on tullut myös tehokkaampia IEEE 802.11ac -standardia tukevia UniFi AP AC -malleja, joiden saatavuus oli tämän insinöörityön aikaan rajoitettua, eikä niitä näin ollen saanut maahantuojalta.

Kuva 20. UniFi AP LR -tukiasema toiminnassa.

UniFi AP LR -tukiaseman tärkeimmät tekniset ominaisuudet:

- mitat 200 x 200 x 36,5 mm (leveys, syvyys, korkeus)
- paino 290 g (430 g kiinnikkeiden kanssa)
- virrankulutus korkeintaan 6 W
- nopeus 300 Mb/s 2,4 GHz:n taajuudella (2x2 MIMO, 802.11 b/g/n)
- WEP, WPA-Personal ja WPA-Enterprise (WPA/WPA2, TKIP/AES)
- yksi 10/100 Passive PoE RJ45 -liitäntä (44, s. 12).

Tukiasema saa virran Passive PoE-tekniikan avulla, mikä siis tarkoittaa, ettei se tue PoE-standardien mukaista laitteen tunnistusta tai tehon valvontaa. Laitteen mukana tulleen 24 V:n Passive PoE -injektorin avulla tukiasemalle saadaan virta ilman PoE-tekniikkaan kykenevää verkkolaitetta. EdgeRouter X -mallissa on passthrough-ominaisuus, joka mahdollistaa injektorin liittämisen eth0-liitäntään. Ominaisuuden käyttöönoton jälkeen virta kulkisi eth0-liitännän kautta eth4-liitäntään. Näin injektorin avulla voitaisiin syöttää virtaa sekä reitittimelle että eth4-liitäntään kytketylle tukiasemalle.

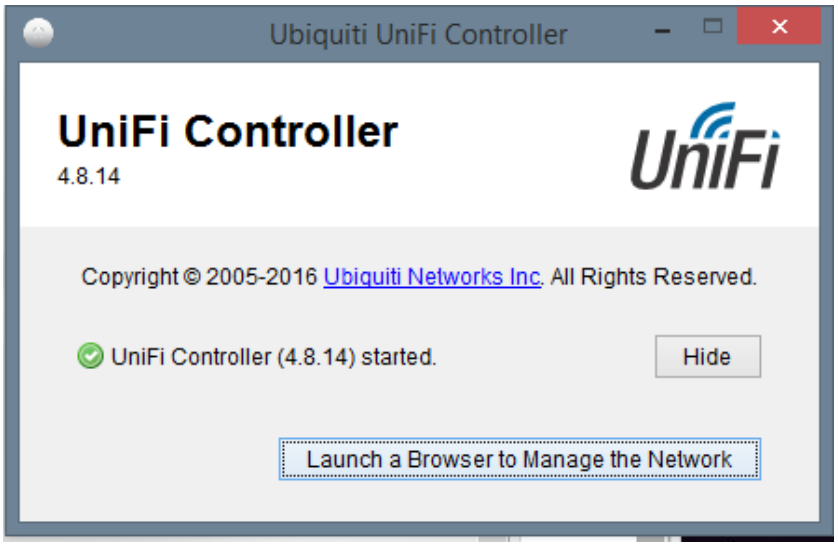
Langattoman tukiaseman verkkoliitännän ja mukana tulleen injektorin maksiminopeus on kuitenkin vain 100 Mb/s. Toteutus hidastaisi 1 Gb/s-nopeuteen kykenevän reitittimen eth0-liitännän 100 Mb/s-nopeuteen ja vaikuttaisi näin kaikkeen reitittimen liikenteeseen. Tällä on vaikutusta oikeastaan vain, jos laajakaistaliittymä kykenee 1 Gb/s-nopeuteen, mikä toistaiseksi ainakin kuluttajaliittymissä on harvinaisempaa. Asialla ei testiympäristössä ollut väliä, mutta yritysympäristössä nopeuden muutos voisi nousta ongelmaksi. (24, s. 2–5; 44, s. 12.)

Kun injektori on kytketty verkkovirtaan, tukiasemaan syttyy oranssi LED-valo (Light-Emitting Diode), mikä ilmaisee sen olevan tehdasasetuksilla ja valmiina liitettäväksi kontrolleriin (46).

4.5 UniFi Controllerin asennus ja tukiaseman konfigurointi

Kontrollerista asennetaan uusin, insinöörityön aikaan saatavilla ollut, versio 4.8.14, joka julkaistiin vuoden 2016 helmikuun loppupuolella (47). Työn testiympäristössä kontrolleri asennetaan tietokoneella, jossa on Windows 8.1 -käyttöjärjestelmä ja Javan version 8 päivitys numero 77. Tukiasemat tarvitsevat TCP (Transmission Control Protocol) -portin 8080 avatuksi tietokoneen palomuurista liikennöidäkseen kontrollerin kanssa. Tietokoneen TCP-porttia 8843 käytetään TLS-suojattuun (Transport Layer Security) kirjautumiseen kontrollerin hallintaliittymään. (48.)

Kontrollerin Windows-version asennustiedosto on tavallinen exe-tiedosto, joka asennetaan aivan kuten mikä tahansa muu ohjelma. Asennuksen jälkeen kontrolleri käynnistetään työpöydälle ilmestyneestä pikakuvakkeesta, jossa on UniFi-tukiaseman kuva. Kontrolleria konfiguroidaan pääosin selaimen kautta, ja ainoa käyttöliittymä sen lisäksi on kuvassa 21 nähtävä ikkuna.



Kuva 21. Kontrollerin käynnissä ollessa näkyvillä oleva ikkuna.

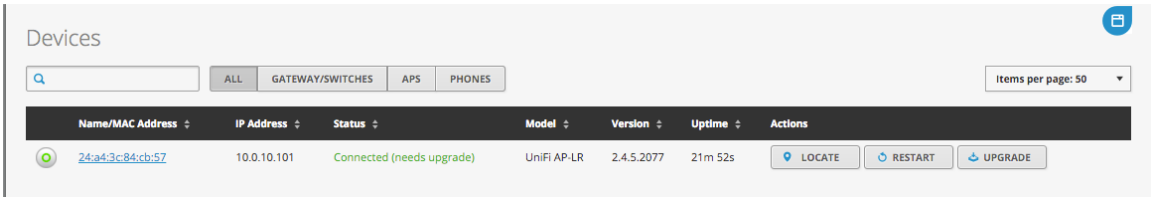
Kontrollerin asetuksien määrittelyä jatketaan käyttöönottoapurilla selaimen kautta. Käyttöönottoapurin ensimmäisessä vaiheessa määritellään maa ja aikavyöhyke. Oikean ajan määrittäminen on erityisen tärkeää kontrollerin lokitapahtumien kirjaamisessa. Kontrolleri yrittää automaattisesti tunnistaa UniFi-laitteita samassa siirtokerroksessa. Tunnistetut laitteet listataan käyttöönottoapurin vaiheessa 2 (kuva 22).

Kuva 22. Samassa verkossa olevat UniFi-laitteet tunnistetaan automaattisesti.

Kolmannessa vaiheessa on mahdollista määritellä suojattu langaton verkko ja avoin vierailijaverkko. Jätin tämän vaiheen väliin, koska halusin määrittää molempiin verkkoihin salauksen. Neljännessä vaiheessa valitaan kontrollerin pääkäyttäjän nimi ja salasana. Tunnuksella pääsee jatkossa kirjautumaan myös SSH-yhteydellä kaikkiin kontrolleriin liitettyihin laitteisiin (49). Vaiheessa 5 esitetään vain yhteenveto käyttöönottoapurilla määritellyistä asetuksista.

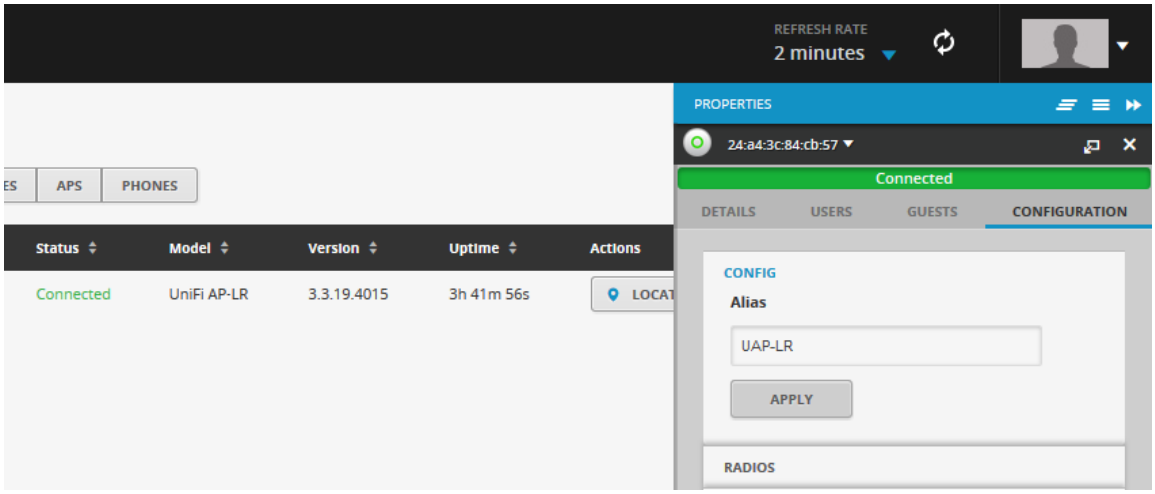
Tukiaseman firmwaren päivitys ja asetukset

Uuden kontrolleriohjelmistoversion mukana toimitetaan aina hallinnoitavien laitteiden uusimmat firmware-päivitykset, jotka voidaan halutessa ladata myös erillisinä tiedostoina (50). Toteutuksessa käytetty UniFi AP LR -tukiasema voidaan päivittää versiosta 2.4.5.2077 versioon 3.3.19.4015 (47). Päivitys suoritetaan kontrollerin laitteiden hallintaosiosta (Devices) painamalla laitteen tietojen perässä sijaitsevaa Upgrade-painiketta (kuva 23). Nähtävissä on myös laitteen MAC-osoite, IP-osoite, toiminnallinen tila, malli, firmwaren versionumero ja viimeisestä käynnistyksestä kulunut aika.



Kuva 23. UniFi AP LR -tukiaseman tiedot laitteiden hallintaosiossa.

Tukiaseman tunnistettavuutta verkossa helpotetaan lisäämällä sille isäntänimi. Toteutuksen pieni laajuus huomioon ottaen tukiasemalle annetaan yksinkertaisesti sen mallia kuvaava nimi eli UAP-LR (kuva 24). Tuotantoympäristössä, jossa laitteita saattaa olla kymmeniä, on tärkeää noudattaa loogista nimeämistä. Yhtenä nimeämiskäytäntönä voidaan käyttää laitteiden fyysistä sijaintia. Neuvotteluhuoneeseen sijoitetulle laiteelle annettaisiin nimeksi Neuvotteluhuone.



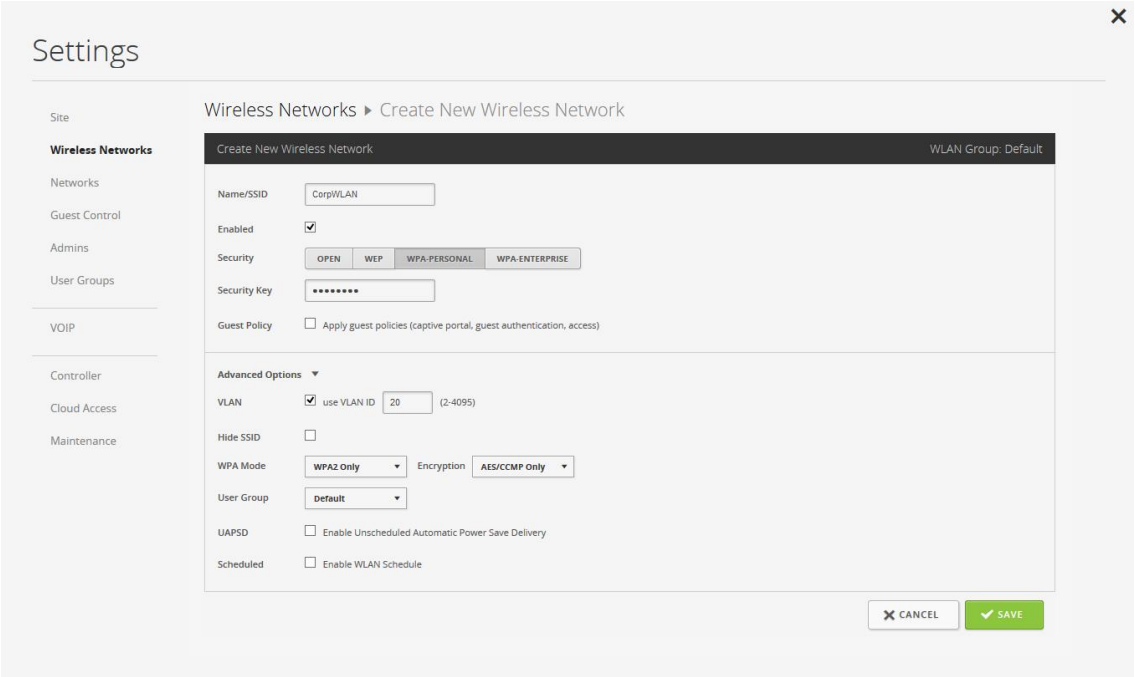
Kuva 24. Tukiaseman isäntänimen asettaminen.

Langattomien verkkojen konfigurointi

Tukiaseman langattomat verkot konfiguroidaan kontrollerin asetuksista *Wireless Networks* -osiosta. Yhtä tukiasemaa kohden on mahdollista konfiguroida enintään neljä SSID:tä (Service Set Indentifier) (44, s. 12). WLAN-ryhmien (WLAN Groups) avulla voidaan kuitenkin luoda useita neljän langattoman verkon ryhmiä, johon voidaan liittää eri tukiasemia. Tukiasemat kuuluvat automaattisesti ainakin yhteen ryhmään nimeltään Default. Lisäasetuksista voidaan määritellä käyttöön WPA tai WPA2. Salaukseksi on mahdollista valita TKIP, AES/CCMP tai automaattinen määritys näiden kahden väliltä päätelaitteen ominaisuuksien mukaan.

Työntekijäverkon asetukset

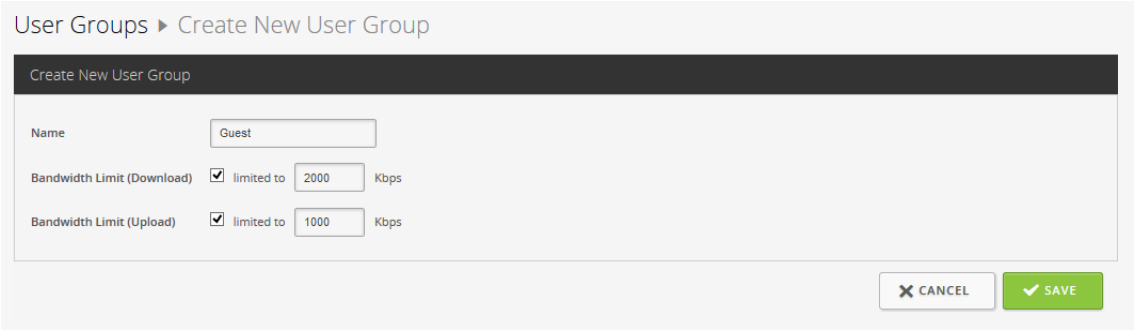
Asetin työntekijäverkon nimeksi CorpWLAN (kuva 25). Suojausmenetelmäksi valitsin WPA-Personal, joka tarkoittaa oletuksena WPA2/PSK-todennusta ja AES/CCMP-salausta. Verkolle asetetaan vahva salasana. Lisäasetuksista määritellään verkolle VLAN-tunniste 20. (38, s. 20–21.)



Kuva 25. Työntekijäverkon asetukset.

Vierailijaverkon asetukset

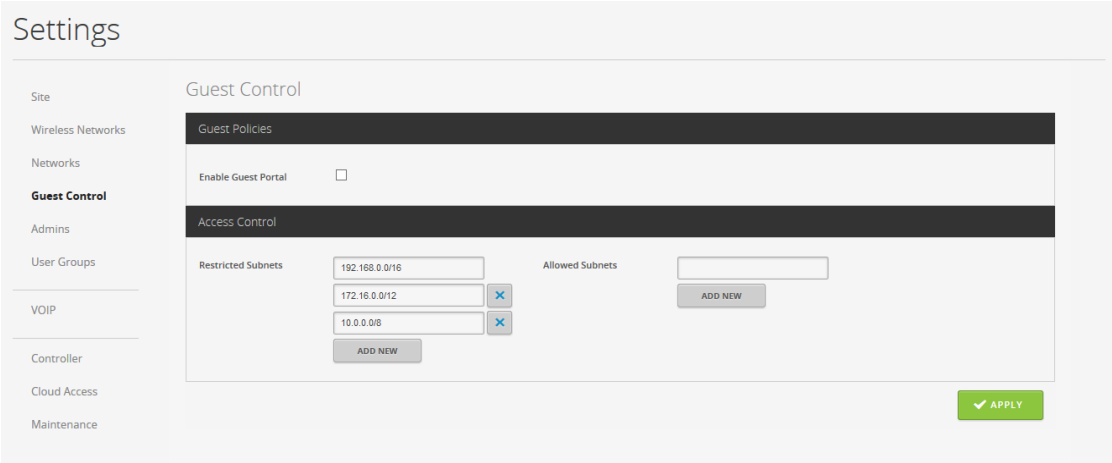
Vierailijaverkolle luodaan oma käyttäjäryhmä (User Group) nimeltä Guest, jolle määritellään tarkat lähetys- ja latausnopeudet. Latausnopeus rajoitetaan 2 Mb:iin/s ja lähetysnopeus 1 Mb:iin/s (kuva 26). Nopeudet riittävät tavalliseen verkkoselailuun ja sähköpostien lukemiseen.



Kuva 26. Uuden käyttäjäryhmän luominen Käyttäjäryhmät-osiosta.

Tarkemmat vierailijaverkkoa koskevat asetukset löytyvät *Guest Control* -osiosta, josta on mahdollista ottaa käyttöön myös vierailijaportaali (kuva 27). Vierailijaportaali on muun muassa lentokentillä ja hotelleissa yleisesti käytetty langattoman verkon kirjau-

tumissivu, jossa on hyväksyttävä käyttöehdot ennen verkkoon liittymistä. *Access Control* -asetuksista on jo valmiiksi rajoitettu pääsy kaikkiin yksityisiin IP-osoitealueisiin: 192.168.0.0/16, 172.16.0.0/12 ja 10.0.0.0/8.

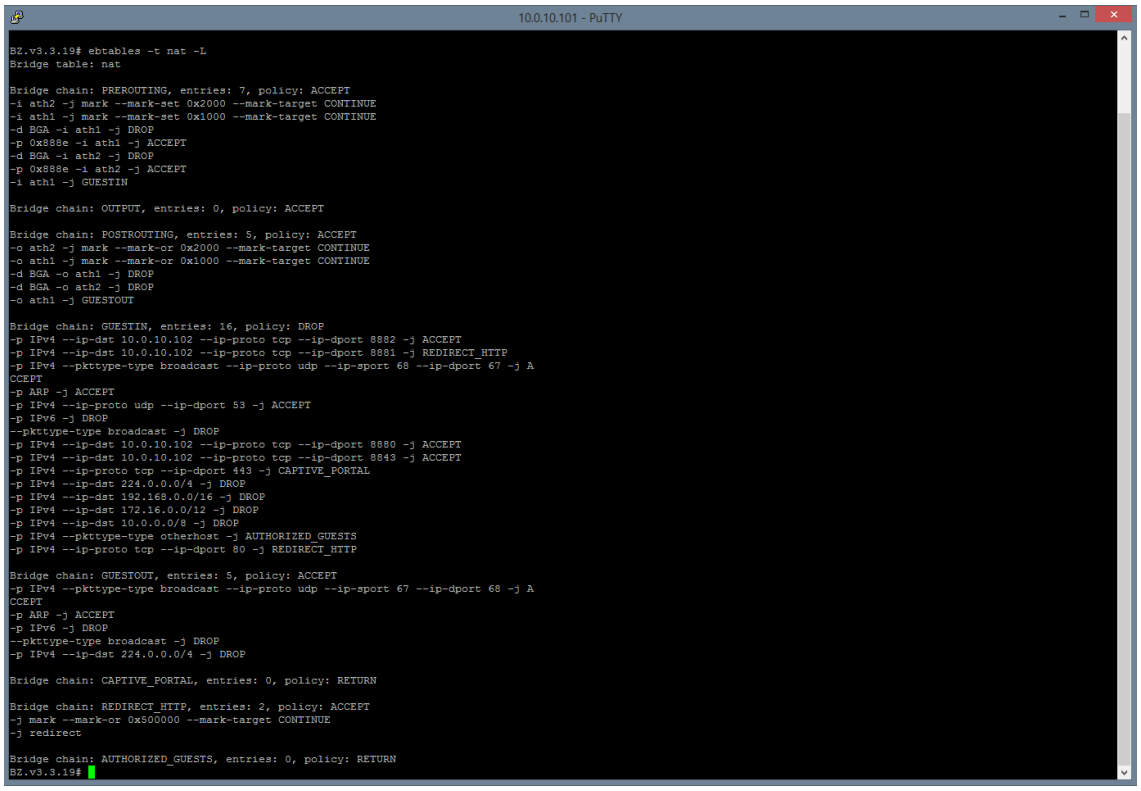


Kuva 27. Guest Control -asetukset.

Alun perin tutkin vierailijaverkon eristyksen toteuttamista reitittimessä palomuurisääntöjen avulla, mutta lopulta totesin kontrollerin tarjoaman ratkaisun olevan tehokkaampi ja helpommin käyttöönotettava. En löytänyt mistään virallista dokumentaatiota tavasta, jolla *Access Control* -ominaisuus on teknisesti toteutettu. Tutkimalla Ubiquitin keskustelupalstaa löysin lopulta viestiketjun, jossa kerrottiin, että ominaisuus toteutetaan tukiasemassa eräänlaisena palomuuriratkaisuna (51). Koska tukiasemaan on asennettu Linux-käyttöjärjestelmä, ominaisuuden tekemät määrittelyt saadaan näkyviin yhdistämällä laitteeseen SSH-yhteydellä ja antamalla komennon

```
ebtables -t nat -L
```

Komennon tuloste nähdään kuvasta 28.

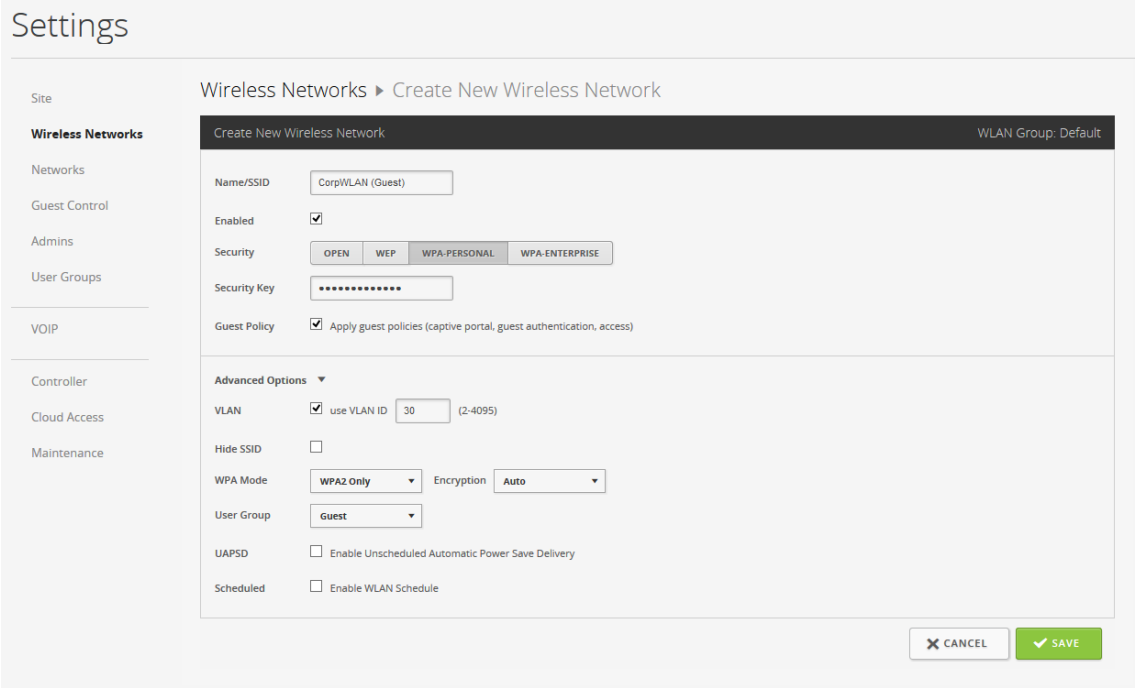


Kuva 28. Access Control -ominaisuuden tekemät määrittelyt tukiasemassa.

Vierailijaverkon SSID ja salaus

Vierailijaverkon tarkoitus on tarjota yrityksen vieraille ja yhteistyökumppaneille helppo pääsy Internetiin. Yrityksen sisäiset tietoturvapolitiikat saattavat määrittää, että työntekijöiden on käytettävä AES-salausta tukevia laitteita, mutta vierailijoilla voi vielä jostain syystä olla vanhempia päätelaitteita. Tästä syystä vierailijaverkkoon liittyvän päätelaitteen annetaan itse määritellä käytettävä salaus TKIPin ja AESin väliltä, joten valitaan salauksen automaattinen määritys (Auto).

Verkolle asetetaan keskivahva, mutta helposti muistettava salasana. Vierailijaverkon nimeksi määritellään CorpWLAN (Guest). *Guest Policy* -valintaruutu ruksataan, mikä ottaa käyttöön *Access Control* -pääsyrajoitukset. VLAN-tunnisteeksi asetetaan 30 ja käyttäjäryhmäksi aikaisemmin luotu Guest (kuva 29).



Kuva 29. Vierailijaverkon asetukset.

4.6 Verkon toiminnallinen testaus

Lopuksi suoritettiin verkon toiminnallinen testaus. Aluksi testasin reitittimen ulkoisen palomuurin toiminnan suorittamalla porttiskannauksen sitä vastaan. Palomuuri toimi kuten pitääkin eikä vastannut edes ICMP (Internet Control Message Protocol) echo reguest -pakettiin.

Testasin DHCP- ja DNS-palveluiden toiminnan yhdistämällä tietokoneen langalliseen verkkoon ja sen jälkeen molempiin langattomiin verkkoihin. Tietokone sai jokaisesta verkosta oikean IP-osoitteen ja DNS-määrittelyt, ja yhteys Internetiin toimi. Vierailija-verkon eristyksen toteutumista testasin kahdella tavalla. Yhdistin tietokoneen vierailija-verkkoon ja älypuhelimen työntekijäverkkoon, minkä jälkeen lähetin tietokoneelta ICMP echo request -paketin puhelimen IP-osoitteeseen. Kun vierailijaverkon pääsyrajoitukset oli kytketty pois päältä, älypuhelin vastasi pyyntöön ICMP echo reply -paketilla. Pääsyrajoitusten ollessa toiminnassa, älypuhelin ei vastannut, joten voidaan todeta verkon olevan erillään muista.

Toisessa testausvaiheessa yhdistin myös älypuhelimen vierailijaverkkoon ja lähetin sille uudelleen ICMP echo request -paketin tietokoneelta. Puhelimen IP-osoite ilmestyi tietokoneen ARP-tauluun (Address Resolution Protocol), mutta MAC-osoite ei. Sama tapahtui myös kokeillessa jotain satunnaista IP-osoitetta. Tästä voidaan todeta eristyksen toteutuvan sekä verkkokerroksella että siirtokerroksella.

Vierailijaverkon nopeuden testaus

Vierailijaverkon nopeutta testattiin Speedtest.net-palvelulla, jossa testipalvelimeksi valittiin Helsingissä sijaitseva DNA:n palvelin. Oman laajakaistaliittymäni nopeus on 50/50 Mb/s. Suoritin testin langattomaan vierailijaverkkoon kytketyltä tietokoneelta. Testin tulokset nähdään kuvasta 30.

Kuva 30. Speedtest.net-palvelulla saadut tulokset vierailijaverkolle.

Vierailijaverkolle saatu vastaanotto- ja lähetysnopeus vastasivat tehtyjä määrittelyjä, joten kaistanrajoitus toimii oikein.

5 Yhteenveto

Insinöörityössä tutustuttiin verkkolaitevalmistaja Ubiquiti Networksiin ja sen tuoteperheisiin. Yrityksellä on laaja valikoima tuotteita eri käyttötarkoituksiin, joiden hinnat on onnistuttu pitämään alhaisena luopumalla raskaasta myyntikoneistosta ja luottamalla asiakkaiden suusta suuhun -markkinointiin. Raportissa tutkittiin UniFi AP LR -tukiaseman ja EdgeRouter X -reitittimen käyttöönottoa ja hallintaa toteuttamalla kuvitteelliselle yritykselle sisäverkko, johon kuului langallisen verkon lisäksi langaton työntekijäverkko ja eristetympi vierailijaverkko. Reitittimeen on asennettu EdgeOS-käyttöjärjestelmä, joka on muunnos Debian/GNU Linuxiin pohjautuvasta Vyatta-käyttöjärjestelmästä. Käyttöjärjestelmän konfiguroiminen komentoriviliittymän kautta muistuttaa Juniperin Junos-käyttöjärjestelmän toimintaa. Reitittimessä on monipuoliset ominaisuudet ja tuet yleisimmille protokollille, joista lähes kaikki ovat konfiguroitavissa web-käyttöliittymän avulla. Reitittimen käyttöönottoapurilla pystytään nopeasti konfiguroimaan riittävät ja tietoturvalliset perusasetukset.

UniFi AP LR -tukiaseman konfigurointiin käytettiin UniFi Controlleria, joka on Java-kielellä ohjelmoitu UniFi-laitteiden hallintaan ja konfigurointiin tarkoitettu verkonhallintajärjestelmä. Kontrolleria on markkinoitu ohjelmisto-ohjattuna verkkoratkaisuna, mutta ohjaus- ja tiedonvälityskerros toteutetaan edelleen laitteissa itsessään. Laitteiden liikennettä ei myöskään tunneloida kontrollerille, joten sen ei tarvitse olla jatkuvasti käynnissä ellei käytössä ole vierailijaportaalia. Langattomien verkkojen salaus toteutettiin WPA2/PSK-todennuksella ja AES/CCMP-salauksella, jotka raportin alussa todettiin tietoturvallisiksi. Kontrollerin Access Control -ominaisuudella voidaan nopeasti toteuttaa verkon eristys verkko- ja siirtokerroksessa.

Laitteiden käyttöönotto vaatii jonkin verran teknistä tuntemusta. Perinpohjaista tutustumista laitteisiin vaikeutti niiden vajavainen ja hajallaan oleva dokumentaatio. Tästä syystä raportissa hyödynnettiin muun muassa Vyatta-käyttöjärjestelmän versioon 6.3 liittyvää dokumentaatiota. Jatkokehityksenä voitaisiin luoda pelkästään UniFi-laitteista koostuva verkko, jossa olisi reitittimiä, kytkimiä ja tukiasemia. EdgeRouter-reitittimestä löytyy monipuolinen IPv6-tuki, joten siihen liittyviä toteutuksia voitaisiin tutkia. Langattoman verkon käyttäjät on mahdollista todentaa 802.1X-standardin mukaisesti esimerkiksi RADIUS-palvelimella. RADIUS-palvelimen avulla kirjautumiseen käytettyjen tunnusten hallinta voitaisiin keskittää. Näin langattoman verkon salasanaa ei tarvitse muuttaa, jos esimerkiksi yksittäinen työntekijä lähtee yrityksestä.

Työn tekeminen oli mielenkiintoista ja pääsin yhdistelemään tietämystäni tietoverkoista, tietoturvasta ja Linuxista. Ubiquitin tuotteet ovat tehokkaita ja monipuolisia, ja niissä riittää varmasti tutkittavaa vielä moneen insinöörityöhön.

Lähteet

1 Mäkipelto, Olli. 2016. Toimitusjohtaja, Noyra Oy. Sähköpostikeskustelu insinöörityö-aiheesta. 4.2.2016.

2 WISP - Nettiyhteys langattomasti kuituverkosta. 2012. Verkkodokumentti. Keskikaista. <http://keskikaista.fi/fi/wisp>. Luettu 4.4.2016.

3 Jaakkohuhta, Hannu. 2005. Lähiverkot. Helsinki: IT-Press.

4 Coleman, David D & Westcott, David A. 2014. CWNA Certified Wireless Network Administrator Official Deluxe Study Guide 4th Edition. Indiana: John Wiley & Sons.

5 Software-Defined Networking: The New Norm for Networks. 2012. Verkkodokumentti. Open Networking Foundation. <https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf>. Luettu 11.4.2016.

6 What's Software-Defined Networking (SDN)? 2013. Verkkodokumentti. SDxCentral. <https://www.sdxcentral.com/resources/sdn/what-the-definition-of-software-defined-networking-sdn/>. Luettu 11.4.2016.

7 Estrada, Pablo. 4 Things You Need to Know About 802.11ac. 2013. Verkkodokumentti. Cisco Meraki Blog. <https://meraki.cisco.com/blog/2013/08/4-things-you-need-to-know-about-802-11ac/>. Luettu 16.4.2016.

8 What is the difference between active and passive PoE? 2015. Verkkodokumentti. OSI CCTV. <https://osicctv.wordpress.com/2015/06/25/what-is-the-difference-between-active-and-passive-poe/>. Luettu 17.4.2016.

9 Non-standard PoE. 2016. Verkkodokumentti. Black Box Corporation. <https://www.blackbox.com/us/products/black-box-explains/non-standard-poe>. Luettu 17.4.2016.

10 Duberstein, Billy. Why Ubiquiti Networks Could Be Legendary. 2015. Verkkodokumentti. <http://seekingalpha.com/article/3664796-ubiquiti-networks-legendary>. Luettu 23.2.2016.

11 UBNT Income Statement. 2016. Verkkodokumentti. Yahoo! Finance. <https://finance.yahoo.com/q/is?s=UBNT&annual>. Luettu 8.3.2016.

12 Ubiquiti Networks, Inc. Stock. 2016. Verkkodokumentti. Yahoo! Finance. <https://finance.yahoo.com/q/pr?s=UBNT+Profile>. Luettu 4.3.2016.

13 Creating Connectivity. 2013. Verkkodokumentti. Leaders Magazine. <http://www.leadersmag.com/issues/2013.4_Oct/PDFs/LEADERS-Robert-Pera-Ubiquiti-Networks-Memphis-Grizzlies.pdf>. Luettu 5.2.2016.

14 Boudway, Ira. The Kid That Bought the Grizzlies. 2013. Verkkodokumentti. <http://www.bloomberg.com/bw/articles/2013-04-24/robert-pera-the-kid-that-bought-the-grizzlies#p2>. Luettu 21.2.2016.

15 Meek, Andy. Apple Taught Ubiquiti's Robert Pera About Perfect Organisms, Now He Owns The Memphis Grizzlies. 2012. Verkkodokumentti. Fast Company. <http://www.fastcompany.com/3003767/apple-taught-ubiquitis-robert-pera-about-perfect-organisms-now-he-owns-memphis-grizzlies>. Luettu 21.2.2016.

16 Pera, Robert. A Look into Ubiquiti's R&D Strategy: Introducing mFI. 2012. Verkkodokumentti. <http://www.rjpblog.com/2012/06/28/a-look-into-ubiquitis-rd-strategy-introducing-mfi-2/>. Luettu 21.2.2016.

17 Broadband. 2016. Verkkodokumentti. Ubiquiti Networks, Inc. <https://www.ubnt.com/broadband/>. Luettu 26.4.2016.

18 Products. 2015. Verkkodokumentti. Ubiquiti Networks, Inc. <https://www.ubnt.com/products/>. Luettu 14.3.2016.

19 Enterprise. 2016. Verkkodokumentti. Ubiquiti Networks, Inc. <https://www.ubnt.com/enterprise/>. Luettu 26.4.2016.

20 UniFi VoIP Phone. 2016. Verkkodokumentti. Ubiquiti Networks, Inc. <https://www.ubnt.com/unifi-voip/uvp/>. Luettu 17.4.2016.

21 EdgeOS - Openflow support. 2012. Verkkodokumentti. Ubiquiti Networks Community. <https://community.ubnt.com/t5/EdgeMAX/EdgeOS-Openflow-support/m-p/312949#M466>. Luettu 17.4.2016.

22 EdgeOS User Guide Release 1.8. 2016. Verkkodokumentti. Ubiquiti Networks. <https://dl.ubnt.com/guides/edgemax/EdgeOS_UG.pdf>. Luettu 4.3.2016.

23 EdgeRouter Datasheet. 2014. Verkkodokumentti. Ubiquiti Networks, Inc. <https://dl.ubnt.com/datasheets/edgemax/EdgeRouter_DS.pdf>. Luettu 6.3.2016.

24 EdgeRouter X Datasheet. 2015. Verkkodokumentti. Ubiquiti Networks, Inc. <https://dl.ubnt.com/datasheets/edgemax/EdgeRouter_X_DS.pdf>. Luettu 8.3.2016.

25 EdgeOS feature backends. 2015. Verkkodokumentti. Ubiquiti Networks Support and Help Center. <http://help.ubnt.com/hc/en-us/articles/204976314-EdgeMAX-EdgeOS-feature-backends>. Luettu 4.3.2016.

26 To which version of Vyatta Core does EdgeOS correspond? 2013. Verkkodokumentti. Ubiquiti Networks Community. <https://community.ubnt.com/t5/EdgeMAX/To-which-version-of-Vyatta-Core-does-EdgeOS-correspond/m-p/501867#M11115>. Luettu 14.3.2016.

27 Timeline of Vyatta. 2015. Verkkodokumentti. VyOS Wiki. <http://vyos.net/wiki/Vyatta>. Päivitetty 25.2.2015. Luettu 14.3.2016.

28 Configuring advanced functionality in the Ubiquiti EdgeRouter Lite. 2014. Verkkodokumentti. 404 Tech Support. <https://www.404techsupport.com/2014/01/configuring-advanced-functionality-in-the-ubiquiti-edgerouter-lite/>. Luettu 14.4.2016.

29 Add other Debian packages to EdgeOS. 2015. Verkkodokumentti. Ubiquiti Networks Support and Help Center. <http://help.ubnt.com/hc/en-us/articles/205202560-EdgeMAX-Add-other-Debian-packages-to-EdgeOS>. Luettu 4.3.2016.

30 BusyBox - The Swiss Army Knife of Embedded Linux. 2008. Verkkodokumentti. Busybox.com. <https://busybox.net/downloads/BusyBox.html>. Luettu 14.2.2016.

31 EdgeMAX EdgeRouter software release v1.8.0. 2016. Verkkodokumentti. Ubiquiti Networks Community. <http://community.ubnt.com/t5/EdgeMAX-Updates-Blog/EdgeMAX-EdgeRouter-software-release-v1-8-0/ba-p/1490756>. Luettu 6.3.2016.

32 What is the root account password? 2015. Verkkodokumentti. Ubiquiti Networks Support and Help Center. <http://help.ubnt.com/hc/en-us/articles/204961724-EdgeMAX-What-is-the-root-account-password->. Luettu 20.2.2016.

33 Roderos, Andrew. Ubiquiti's EdgeOS CLI Introduction. 2016. Verkkodokumentti. <http://networkjutsu.com/edgeos-cli-introduction/>. Luettu 14.4.2016.

34 Does allowing telnet and rlogin increase the risk to my site? 2015. Verkkodokumentti. SANS Institute. <https://www.sans.org/security-resources/idfaq/telnet_rlogin.php>. Luettu 20.2.2016.

35 EdgeMAX - Zone-Policy CLI Example. 2016. Verkkodokumentti. Ubiquiti Networks Support and Help Center. <http://help.ubnt.com/hc/en-us/articles/204952154-EdgeMAX-Zone-Policy-CLI-Example>. Luettu 14.4.2016.

36 Firewall Reference Guide. 2011. Verkkodokumentti. Vyatta, Inc. <https://dl.networklinx.com/vyatta/6.3/Vyatta_Firewall_R6.3_v01.pdf>. Luettu 9.4.2016.

37 Layman's firewall explanation. 2015. Verkkodokumentti. Ubiquiti Networks Community. <https://community.ubnt.com/t5/EdgeMAX/Layman-s-firewall-explanation/m-p/1436103#M91494>. Luettu 14.4.2016.

38 UniFi Controller User Guide. 2016. Verkkodokumentti. Ubiquiti Networks, Inc. <https://dl.ubnt.com/guides/UniFi/UniFi_Controller_V4_UG.pdf>. Luettu 4.3.2016.

39 UniFi - What protocol does the controller use to communicate with the UAP? 2016. Verkkodokumentti. Ubiquiti Networks Support and Help Center.

<http://help.ubnt.com/hc/en-us/articles/204976094-UniFi-What-protocol-does-the-controller-use-to-communicate-with-the-UAP->. Luettu 29.2.2016.

40 The new EdgeRouter X and EdgeRouter X SFP. 2015. Verkkodokumentti. Ubiquiti Networks Community. <https://community.ubnt.com/t5/EdgeMAX/The-new-EdgeRouter-X-and-EdgeRouter-X-SFP/m-p/1222426#M61976>. Luettu 17.4.2016.

41 EdgeMAX - Ubiquiti Networks Store. 2016. Verkkodokumentti. <https://store.ubnt.com/edgemax.html>. Luettu 7.4.2016.

42 List of routing config settings that are no longer supported. 2016. Verkkodokumentti. Ubiquiti Networks Community. <http://community.ubnt.com/t5/EdgeMAX/v1-8-0-List-of-routing-config-settings-that-are-no-longer/m-p/1493179#M99501>. Luettu 19.3.2016.

43 EdgeMAX - Upgrading EdgeOS firmware. 2015. Verkkodokumentti. Ubiquiti Networks Support and Help Center. <http://help.ubnt.com/hc/en-us/articles/205146110-EdgeMAX-Upgrading-EdgeOS-firmware>. Luettu 9.4.2016.

44 UniFi AP LR Datasheet. 2015. Verkkodokumentti. Ubiquiti Networks, Inc. <https://dl.ubnt.com/datasheets/unifi/UniFi_AP_DS.pdf>. Luettu 10.3.2016.

45 UniFi AP Long-Range. 2016. Verkkodokumentti. Ubiquiti Networks Store. <https://store.ubnt.com/unifi/unifi-ap-118.html>. Luettu 17.4.2016.

46 UniFi - What do the LED Color Patterns Represent for UniFi Devices? 2015. Verkkodokumentti. Ubiquiti Networks Support and Help Center. <http://help.ubnt.com/hc/en-us/articles/204910134-UniFi-What-do-the-LED-Color-Patterns-Represent-for-UniFi-Devices->. Luettu 12.4.2016.

47 UniFi 4.8.14 is released. 2016. Verkkodokumentti. Ubiquiti Networks Community. <https://community.ubnt.com/t5/UniFi-Updates-Blog/UniFi-4-8-14-is-released/ba-p/1495935>. Luettu 16.3.2016.

48 UniFi - Change Default Ports for Controller and UAPs. 2016. Verkkodokumentti. Ubiquiti Networks Support and Help Center. <http://help.ubnt.com/hc/en-us/articles/204910084-UniFi-Change-Default-Ports-for-Controller-and-UAPs>. Luettu 29.2.2016.

49 UniFi - What is the default username / password for UAPs and controller? 2016. Verkkodokumentti. Ubiquiti Networks Support and Help Center. <http://help.ubnt.com/hc/en-us/articles/204909374-UniFi-What-is-the-default-username-password-for-UAPs-and-controller->. Luettu 18.4.2016.

50 UniFi - How do I update the firmware? 2015. Verkkodokumentti. Ubiquiti Networks Support and Help Center. <http://help.ubnt.com/hc/en-us/articles/204949744-UniFi-How-do-I-update-the-firmware->. Luettu 14.2.2016.

51 UAP Guest Access Control (Restricted/Allowed Subnets). 2015. Verkkodokumentti. Ubiquiti Networks Community. <https://community.ubnt.com/t5/UniFi-Wireless/UAP-Guest-Access-Control-Restricted-Allowed-Subnets/m-p/1320447#M115632>. Luettu 14.4.2016.

EdgeRouter X -reitittimen konfiguraatio

Käyttöönottoapurin ja manuaalisten määrittelyjen tuottama lopullinen reitittimen konfiguraatio:

```
firewall {
    all-ping enable
    broadcast-ping disable
    ipv6-receive-redirects disable
    ipv6-src-route disable
    ip-src-route disable
    log-martians enable
    name WAN_IN {
        default-action drop
        description "WAN to internal"
        rule 10 {
            action accept
            description "Allow established/related"
            state {
                established enable
                related enable
            }
        }
        rule 20 {
            action drop
            description "Drop invalid state"
            state {
                invalid enable
            }
        }
    }
    name WAN_LOCAL {
        default-action drop
        description "WAN to router"
        rule 10 {
            action accept
```

```
            description "Allow established/related"
            state {
                established enable
                related enable
            }
        }
        rule 20 {
            action drop
            description "Drop invalid state"
            state {
                invalid enable
            }
        }
    }
    receive-redirects disable
    send-redirects enable
    source-validation disable
    syn-cookies enable
}
interfaces {
    ethernet eth0 {
        address dhcp
        description Internet
        duplex auto
        firewall {
            in {
                name WAN_IN
            }
            local {
                name WAN_LOCAL
            }
        }
        speed auto
    }
    ethernet eth1 {
        description Local
```

```
    duplex auto
    speed auto
}
ethernet eth2 {
    description Local
    duplex auto
    speed auto
}
ethernet eth3 {
    description Local
    duplex auto
    speed auto
}
ethernet eth4 {
    description Local
    duplex auto
    speed auto
}
loopback lo {
}
switch switch0 {
    address 10.0.10.1/24
    description Local
    mtu 1500
    switch-port {
        interface eth1
        interface eth2
        interface eth3
        interface eth4
    }
    vif 20 {
        address 10.0.20.1/24
        description EMPLOYEE
        mtu 1500
    }
    vif 30 {
```

```
            address 10.0.30.1/24
            description GUEST
            mtu 1500
        }
    }
}
service {
    dhcp-server {
        disabled false
        hostfile-update disable
        shared-network-name EMPLOYEE {
            authoritative disable
            subnet 10.0.20.0/24 {
                default-router 10.0.20.1
                dns-server 10.0.20.1
                lease 86400
                start 10.0.20.100 {
                    stop 10.0.20.254
                }
            }
        }
        shared-network-name GUEST {
            authoritative disable
            subnet 10.0.30.0/24 {
                default-router 10.0.30.1
                dns-server 8.8.8.8
                lease 86400
                start 10.0.30.100 {
                    stop 10.0.30.254
                }
            }
        }
        shared-network-name LAN {
            authoritative disable
            subnet 10.0.10.0/24 {
                default-router 10.0.10.1
```

```
                dns-server 10.0.10.1
                lease 86400
                start 10.0.10.100 {
                    stop 10.0.10.254
                }
            }
        }
    }
    dns {
        forwarding {
            cache-size 150
            listen-on switch0
            listen-on switch0.20
        }
    }
    gui {
        https-port 443
    }
    nat {
        rule 5010 {
            description "masquerade for WAN"
            outbound-interface eth0
            type masquerade
        }
    }
    ssh {
        port 22
        protocol-version v2
    }
}
system {
    host-name ERX
    login {
        user admin1 {
            authentication {
                encrypted-password ****************
```

```
                plaintext-password ****************
            }
            full-name ""
            level admin
        }
    }
    ntp {
        server 0.ubnt.pool.ntp.org {
        }
        server 1.ubnt.pool.ntp.org {
        }
        server 2.ubnt.pool.ntp.org {
        }
        server 3.ubnt.pool.ntp.org {
        }
    }
    syslog {
        global {
            facility all {
                level notice
            }
            facility protocols {
                level debug
            }
        }
    }
    time-zone Europe/Helsinki
}
```